COMMENT

BUILDING A COMMUNITY THROUGH WORKPLACE E-MAIL: THE NEW PRIVACY FRONTIER

Peter Schnaitman[*]

Cite As: Peter Schnaitman, Comment, *Building a Community Through Workplace E-mail: The New Privacy Frontier*, 5 MICH. TEL. TECH. L. REV. 177 (1999) <http://www.mttlr.org/schnaitman.pdf>.

[*] J.D. Candidate, Case Western Reserve University School of Law, 1999; B.A. Earlham College, 1992. The author would like to thank Professor Paul M. Schwartz for his comments and criticisms, and Christa Hohmann for her support, understanding, and input.

I. INTRODUCTION

"If you've got a boss who is monitoring e-mail to see if people are calling him a jerk—he probably is . . . ."[1]

The relatively new technology of electronic mail (e-mail) presents an entirely new issue of workplace privacy. Currently, whether a person has a privacy interest in their workplace e-mail communications is as unsettled an issue as it has been since the technology emerged in the early part of this decade as the preferred mode of communication in the workplace. Indeed, e-mail may soon be the preferred mode of communication in general.[2]

This comment will argue that all e-mail users have a privacy interest in workplace e-mail communications and that the current law does not afford e-mail users any type of protection for this interest. Part I will address the rise of e-mail in the workplace and the privacy interest users have in their workplace e-mail. Part II will discuss the law currently in existence that has been applied to workplace e-mail privacy and how this body of law has failed to recognize a privacy interest in workplace e-mail messages. Part III will discuss the few solutions that have been proposed to deal with workplace e-mail privacy and how these fall far short of protecting this important privacy interest. This comment will then propose a structure of federal legislation to address this issue, concluding that e-mail in the workplace should be a protected privacy interest and that federal legislation is the only way in which to protect this interest.

---

1. Abdon M. Pallasch, *Company Policies to Monitor E-mail Licking Edge of Electronic Envelope*, CHICAGO LAWYER, August 1995, at 4.

2. "[A]nother recent survey, according to a 1996 Dickinson Wright law firm newsletter, estimates there will be 72 million employees using e-mail to send 4.1 trillion messages." Kathleen Sibley, *The E-mail Dilemma: To Spy or Not to Spy*, COMPUTING CANADA, March 31, 1997 at 14. "E-mail is in use, in some capacity, in all Fortune 1000 companies, and it is expected that by the year 2000, 40 million e-mail users will be sending 60 billion e-mail messages a year." Steven Miller, *E-mail's Popularity Poses Workplace Privacy Problems*, BUSINESS FIRST OF COLUMBUS, Oct. 3, 1997, at 15. *See also* Hal Berghel, *E-mail—The Good, the Bad, and the Ugly*, COMMUNICATIONS OF THE ACM, April 1, 1997 at 11.

II. E-MAIL AND PRIVACY

A. *The Technology of E-mail and its Current Uses*

E-mail is a powerful communications tool. Statistics abound about the current use of e-mail in the business setting.[3] It has been reported that in business settings e-mail is used more often than postal mail.[4] While e-mail is now used most frequently in business settings, its use by people for non-business conversation is only expected to increase and in the future e-mail may be the preferred mode of communication for most people.[5] E-mail differs from other forms of office communication technology because of three factors: the ease of use of e-mail software, the permanency of e-mail messages, and the ability to use e-mail as more than just another communication device. These three new capabilities of e-mail and the prevalence of e-mail are the reasons why the technology of e-mail communication raises unique new issues of workplace privacy.

The use of e-mail in the workplace is obvious to most people. It allows a user to type a message in a controlled manner and to review the message prior to sending it.[6] It also allows the receiver of the message to read messages at his convenience. Furthermore, e-mail allows a user to easily send the same message to many people at once, to forward messages to other people, or to reply to a message from another person.[7] Since a copy of the e-mail message is stored in the user's log, he can access the message again for future reference. These are some of e-mail's advantages over postal mail and telephone conversations.

However, most e-mail users do not recognize the permanency of e-mail messages. E-mail servers store e-mail messages even after a user has downloaded the message onto their personal computer. These messages stored on the server are then backed up in a more permanent way, by being stored on magnetic tape. These back-ups are of the entire system, not just the e-mail messages, and their primary purpose is to aid the system operator in case the system crashes and must be restored. Most

3. "In the United States today there are close to 20 million electronic mail ("[e]-mail") users . . . . It is projected that there will be more than 40 million [e]-mail users nationwide by the year 2000 . . . . Today, 90 percent of all companies with more than 1,000 employees use [e]-mail." Anthony J. Dreyer, Note, *When the Postman Beeps Twice: The Admissibility of Electronic Mail Under the Business Records Exception of the Federal Rules of Evidence*, 64 FORDHAM L. REV. 2285, 2288 (1996).

4. *See* Amie M. Soden, *Protect Your Corporation from E-mail Litigation: Privacy, Copyright Issues Should Be Addressed in Policy*, CORPORATE LEGAL TIMES, May 1995, at 19; Dreyer, *supra* note 3, at 2288.

5. *See* Dreyer, *supra* note 3, at 2288.

6. *See* Berghel, *supra* note 2, at 11.

7. *See id*.

organizations retain back-up tapes for several years and messages on these tapes, even when overwritten with other data, can easily be accessed and searched to provide access to an entire e-mail message in its original form.[8] The legitimate purpose of back-up has lead to the permanence of e-mail and is the basis for most legal issues surrounding e-mail.[9]

E-mail is a relatively new technology and its uses are still being developed and adapted for use in the workplace. E-mail is not just another method of sending messages and communicating with other people. While it is a way to send messages, it is also a way that information is being digitized, collected, organized and manipulated. E-mail can be a postage letter, a facsimile message, a telephone call, a filing cabinet, a desk drawer, a voice mail system, a client file, a personnel file, or a personal organizer.[10] E-mail is more permanent than even a paper document.[11] E-mail is more accessible than a phone call or a desk. The record created by e-mail is more precise than any communication received through the postal system or from a facsimile machine. These are the factors that make e-mail different and new, and an issue that must be addressed by the law.[12]

8. "[M]ainframe backups also make archiving and retrieving e-mail records much easier than their paper counterparts." Dreyer, *supra* note 3, at 2291.

9. E-mail and its ramifications are in part a result of its permanence. This permanence is a result of the need to backup information stored on computer systems. Issues such as reading e-mail, evidentiary uses of e-mail, and the discovery of e-mail in litigation would not exist were it not for the backing-up of computer systems. Discussing the application of the rules of evidence to e-mail, *see id.* at 2299—2328. *See also* Betty Ann Olmstead, *Electronic Media: Management and Litigation Issues: When "Delete" Doesn't Mean Delete*, 63 DEF. COUNS. J. 523 (1996).

10. "In today's modern business setting, e-mail messages may include status reports, inventory lists, minutes of meetings, drafts of documents, business strategies, or records of important business decisions." Dreyer, *supra* note 3, at 2289.

11. "Unlike paper documents that can be discarded easily, 'purged' electronic documents may still exist in some sort of archival media where they can stay for an indefinite period of time. Even when archived tapes are removed for reuse and the information has been finally overwritten, such documents may still be recoverable." Olmstead, *supra* note 9, at 526. *See also* Dreyer *supra* note 3, at 2291. "In actuality, most data can be restored unless it has been overwritten . . . and even overwritten documents can be deciphered." Marianne Lavalle, *Digital Information Boom Worries Corporate Counsel: Questions Arise About Data Overload, Online Privacy, the Retrieval of Deleted E-mail and Technological Monopoly*, NAT'L L.J., May 30, 1994, at B1.

12. *See* John Araneo, Note, *Pandora's (E-mail) Box: E-mail Monitoring in the Workplace*, 14 HOFSTRA LAB. L.J. 339, 356 (1996).

B. *Privacy and Workplace E-mail*

1. Conceptions of Privacy

Privacy is a broad right and has been analyzed in many different ways. While the right to privacy has many different aspects and has been analyzed and developed in many different ways, this comment focuses upon the purpose of a privacy interest in workplace e-mail communications and where this interest comes from. Privacy is not an absolute concept, but one which is used to help individuals in society define their community and the "boundaries of community life."[13] Defining communities and the scope of personal conduct in these communities is vital in today's society, because communities and other types of boundaries are increasingly less well defined than they have been in the past due to modern technology's erosion of the boundaries set by the natural barriers of time and geography.

One commentator, Fred H. Cate, has stated that "privacy is a tool needed to achieve some result. A society's interest in protecting privacy reflects that society's interest in the result, not in privacy."[14] Robert C. Post has argued that the tort of invasion of privacy "safeguards the interests of individuals in the maintenance of rules of civility."[15] He asserts that these rules of civility:

> enable individuals to receive and to express respect, and to that extent are constitutive of human dignity . . . . [T]hese rules also enable individuals to receive and to express intimacy, and to that extent are constitutive of human autonomy . . . . [T]he civility rules maintained by the tort embody the obligations owed by members of a community to each other, and to that extent define the substance and boundaries of community life.[16]

This is where the invasion of privacy tort of intrusion comes into play to provide people with a way, according to the terms of Post, "to receive and to express respect."[17] The interest protected is a recognition that personal autonomy must be afforded some measure of standing in the face of the ability of other people in the workplace to access e-mail communications. In the terms of Cate, the result to be achieved for society is the

13. *See* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 31 (Brookings Institution Press 1997); Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 1008 (1989).

14. Cate, *supra* note 13, at 23.

15. Post, *supra* note 13, at 1008.

16. *Id*.

17. *Id*.

protection of personal autonomy in communicating through e-mail and this result equals the privacy interest.[18]

Because there are more e-mail communications and these communications are permanent, not affording a privacy interest to e-mail users in workplace communications means that the user has no way to establish boundaries and then no way to determine what obligations are owed to all members of the workplace community. As Alan Westin has stated:

> Each individual must, within the larger context of his culture, his status, and his personal situation, make a continuous adjustment between his needs for solitude and companionship; for intimacy and general social intercourse; for anonymity and responsible participation in society; for reserve and disclosure.[19]

2. Privacy in the Workplace

Conceptions of the privacy interest of workplace e-mail aside, "private employees have diminished expectations of personal privacy in the modern workplace."[20] One commentator has summarized employee workplace privacy as follows: "[t]raditionally, employees have received little privacy protection on the job."[21] While privacy rights for employees can be found in federal and state constitutions, "[t]he basic legal bulwark for private sector employee privacy protection is the common law of torts, most often through the tort of invasion of privacy."[22]

Prosser listed the elements of the intrusion kind of the invasion of privacy tort as "the intrusion must be something which would be offensive or objectionable to a reasonable man . . . . [T]he thing into which there is prying or intrusion must be, and be entitled to be, private."[23] The Restatement of Torts includes a more modern summarization of these factors: "one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is

---

18. "Privacy is an essential component of individual autonomy and dignity. Our sense of liberty is partly defined by the ability to control our own lives—whether this be the kind of work we undertake, who we choose to associate with, where we live, the kind of religious and political beliefs we hold, or the information we wish to divulge about ourselves." Gary T. Marx & Sanford Sherizen, *Monitoring on the Job: How to Protect Privacy as Well as Property*, TECH. REV., Nov.-Dec. 1986, at 63, 65.

19. ALAN F. WESTIN, PRIVACY AND FREEDOM 42 (1967).

20. John C. Barker, Note, *Constitutional Privacy Rights in the Private Workplace, Under The Federal and California Constitutions*, 19 HASTINGS CONST. L.Q. 1107, 1108 (1992).

21. Steven Winters, Comment, *The New Privacy Interest: Electronic Mail in the Workplace*, 8 HIGH TECH. L.J. 197, 201 (1993).

22. Frank J. Cavico, *Invasion of Privacy in the Private Employment Sector: Tortious and Ethical Aspects*, 30 HOUS. L. REV. 1263, 1266 (1993).

23. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 391 (1960).

subject to liability to the other for invasion of . . . privacy, if the intrusion would be highly offensive to a reasonable person."[24]

In terms of how the tort of invasion of privacy should be applied to cases of e-mail monitoring, one commentator has formulated the question as "whether computer technology has so shifted control to the employer that the scales need to be re-calibrated to better protect an employee's privacy rights."[25] Another primary question that needs to be answered is "whether the employee has a reasonable expectation of privacy in employer-provided computers and e-mail services."[26] There is little debate about the actual questions involved. The debate centers around where to draw the line; or to use the query of Post, how the community of the individual workplace is going to "define the substance and boundaries of community life" and to then clarify "the obligations owed by members of a community to each other."[27]

The traditional view of the issue of workplace privacy, is where the employer's rights begin and the employee's interest in privacy ends. As one commentator has noted, "[i]t is argued that employers' interests should be favored because the work is done on the employers' premises. Employers own the communications equipment used at work and it is the company's business which is being conducted on this equipment."[28] However, a broader approach might be more appropriate. With e-mail and the interest in personal privacy, a tension exists not only between employer and employee, but also between the user and the people with the capability to access the e-mail system. By narrowing the issue to focus solely upon the construct of the employer and employee relationship, the broader question of whether individual users have a privacy interest in their e-mail is ignored.

The privacy interest to be protected, originally identified by Warren and Brandeis, was one belonging to individuals.[29] The technology of e-mail attacks this idea of individual privacy, because e-mail does not just belong to individuals. The e-mail messages of all users can be accessed whether that person is a secretary or the Chief Executive Officer. Computer technologies are equalizers; they destroy previous forms of authority by treating all users equally. For this reason all users' privacy interests must be analyzed as a whole and not based upon titles of

24. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

25. *See* Winters, *supra* note 21, at 202.

26. Brian D. Pedrow & Debra E. Kohn., *Tampering with E-mail: Proprietary Rights and Privacy Issues*, 21 LAW PRAC. MGMT., Nov.-Dec. 1995 at 36, 38.

27. Post, *supra* note 13, at 1008.

28. *See* Winters, *supra* note 21, at 201.

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

authority. E-mail creates a larger community for users beyond that of the workplace and in this larger community are the values that the privacy interest protects.[30]

III. THE LAW

A. *Electronic Communications Privacy Act*

The only federal law currently applicable to the issue of workplace e-mail monitoring is the Electronic Communications Privacy Act of 1986 (ECPA).[31] This Act provides a framework for the discussion of the issue of privacy rights in workplace e-mail. Many of the Act's provisions that apply to workplace e-mail privacy issues remain untested, but some case law has emerged interpreting the applicability of some provisions of the Act. These cases demonstrate how courts may be inclined to apply the ECPA to cases of workplace e-mail privacy, in addition to demonstrating the inherent weaknesses of the ECPA in providing users of workplace e-mail systems with any type of privacy protections.

The ECPA is an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, also known as the Federal Wiretap Law.[32] The 1986 amendment to the statute was to "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies."[33] The Act among other things, provided a federal definition of e-mail and other "new" communication technologies, and brought these technologies into the previous wiretap law of the Omnibus Crime Control and Safe Streets Act of 1968.[34] The primary components of the Act are Title I, which ad-

30. "[M]onitoring could become much more extensive in society at large. Practices developed at work can easily spill over into other areas." Marx, *supra* note 18, at 70.

31. *See* 18 U.S.C. §§ 2510—2711 (1998).

32. *See* S. REP. NO. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555; U.S.C. § 2510 (1998).

33. S. REP. NO. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. at 3555.

34. The Act defined e-mail as:

> Electronic mail is a form of communication by which private correspondence is transmitted over public and private telephone lines. In its most common form, messages are typed into a computer terminal, and then transmitted over telephone lines to a recipient computer operated by an electronic mail company. If the intended addressee subscribes to the service, the message is stored by the company's computer "mail box" until the subscriber calls the company to retrieve its mail, which is then routed over the telephone system to the recipient's computer. If the addressee is not a subscriber to the service, the electronic mail company can put the message onto paper and then deposit it in the normal postal system. Electronic mail systems may be available for public use or may be proprietary, such as systems operated by private companies for internal correspondence.

S. REP. NO. 99-541, at 8 (1986), *reprinted in* 1986 U.S.C.C.A.N. at 3562.

dresses the interception of wire, oral, and electronic communications and Title II, which addresses access to stored communications.[35]

Before the enactment of the Act, studies were done to underscore the need for the Act.[36] One such study was the Office of Technology Assessment's report entitled "Electronic Surveillance and Civil Liberties," which concluded that "current legal protections for electronic mail are 'weak, ambiguous, or non-existent,' and that 'electronic mail remains legally as well as technically vulnerable to unauthorized surveillance.'"[37] Concerning the need for the Act, the Senate committee's report stated:

> A letter sent by first class mail is afforded a high level of protection against unauthorized opening by a combination of constitutional provisions, case law, and U.S. Postal Service statutes and regulations . . . . But there are no comparable Federal statutory provisions to protect the privacy and security of communications transmitted by new noncommon carrier communications services or new forms of telecommunications and computer technology.[38]

The Senate report further stated: "This gap [between postal privacy protections and new technology protections] results in legal uncertainty . . . . It may also discourage American businesses from developing new innovative forms of telecommunications and computer technology."[39]

Although Congress's intention was to resolve the "legal uncertainty" through the enactment of the ECPA, it remains unclear whether this has happened. One commentator has stated that the ECPA "does not complete the work required to be done to provide adequate assurances of electronic privacy,"[40] because:

> [The Act] creates a legal framework that substantially constrains access by government agents to all forms of electronic communications clearly and reasonably intended to be kept private. But the Act does not complete the work required to be done to provide adequate assurance of electronic privacy. Those who provide electronic communications services . . . must make

35. *See* 18 U.S.C. §§ 2510—2522, 2711

36. S. REP. NO. 99-541, at 4 (1986), *reprinted in* 1986 U.S.C.C.A.N. at 3558.

37. *Id.*

38. *Id.* at 5, *reprinted in* 1986 U.S.C.C.A.N. at 3559.

39. *Id.*

40. David Johnson, *Privacy: Good Sysops Should Build Good Fences* (visited Apr. 13, 1998) <http://www.eff.org/pub/Privacy/good_fences_johnson.article>.

> clear which types of messages are to be kept strictly private and which are meant to be freely shared . . . .[41]

To date, the ECPA primarily has been raised in cases of phone interception and has yet to be raised in a case involving workplace e-mail monitoring.[42] A recent case involving e-mail to raise an ECPA claim was *Steve Jackson Games, Inc. v. United States Secret Service*.[43] In *Steve Jackson*, the Fifth Circuit Court of Appeals provided a useful interpretation of the two provisions of the ECPA and their relation to accessing e-mail communications.[44] The district court in *Steve Jackson*, held that Title I of the ECPA had not been violated by the Secret Service's actions because "[the] acquisition of the contents of the electronic communications was not contemporaneous with the transmission of those communications."[45] The court of appeals in affirming the district court's action, discussed at length the difference between the requirements of Title I and Title II.[46] The court concluded that the Secret Service agents' actions were not an "interception" for the purpose of Title I of the statute, but instead were an accessing of stored communications under Title II. The court noted the difference between the procedural safeguards in standards of Title I and II was because:

> Interception thus poses a significant risk that officers will obtain access to communications which have no relevance to the investigation they are conducting. That risk is presented to a lesser degree, and can be controlled more easily, in the context of stored electronic communications, because, as the Secret Service advised the district court, technology exists by which relevant communications can be located without the necessity

41. *Id.*

42. *See* Frank C. Morris, *Issues from the Electronic Workplace E-mail Communications: The Developing Employment Law Nightmare*, SB07 ALI-ABA 335, 341 (1996). *See, e.g.*, Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992) (finding a violation of the ECPA for taping an employee's phone conversations without obtaining her consent); Watkins v. L.M. Berry & Company, 704 F.2d 577 (11th Cir. 1983) (finding that there was a material issue of fact about whether an employee had consented to the employer monitoring the employee's phone calls). However, states have enacted statutes which mirror the ECPA and claims have been raised pursuant to those statutes without success, *see* discussion *infra* Part II.C.

43. Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457 (3d Cir. 1996) (Steve Jackson dealt with the accessing of e-mail messages by the Secret Service on a server that had been seized as part of a raid on a computer bulletin board operator. The plaintiffs were operators of and users of the server which was used for e-mail communications and an electronic bulletin board. Many of the users' e-mail in question had not been read by the users prior to the server's seizure by the Secret Service. The court of appeals affirmed the trial court's holding that Title II of the ECPA had been violated, but not Title I.).

44. *Id.* at 460–64.

45. *Id.* at 459–60.

46. *Id.* at 461–64.

> of reviewing the entire contents of all of the stored communications.[47]

In conclusion, the court stated, "that Congress intended to treat wire communications differently from electronic communications. Access to stored electronic communications may be obtained pursuant to a search warrant, 18 U.S.C. § 2703; but, access to stored wire communications requires a court order pursuant to § 2518."[48] The appeals court found that the Secret Service had violated the provisions of Title II and awarded the plaintiffs damages.[49]

Steve Jackson dealt with the accessing of e-mail by the Secret Service for the purposes of a law enforcement investigation.[50] However, the case demonstrates the difference between the interpretation of an "interception" and a "stored communication" under the ECPA. Because e-mail messages are routed through a server where they are saved, in terms of applying the ECPA to the accessing of e-mail messages Title II will come into play and not Title I.[51]

Title II provides several exceptions to the ECPA's prohibition against accessing electronic communications.[52] The two most important sections for the purpose of workplace e-mail are what have been termed the "business-extension," "business use," or "ordinary course of business" exception (18 U.S.C. § 2701(c)(1)) and the "consent" exception (18 U.S.C. § 2701(c)(2)).[53] While these exceptions exist as part of the law, their parameters have not been tested through cases involving the accessing of stored communications; therefore, most cases defining the scope of the ECPA's exceptions have arisen under Title I.

---

47. *Id.* at 463.

48. *Id.* at 464. *See* discussion *infra* pp. 11–15 (for a discussion about the importance of the court's distinction in Steve Jackson Games that the accessing of an e-mail communication should be analyzed under the prohibitions of Title II of the ECPA not Title I).

49. *Id.* at 464.

50. *See id.* at 463.

51. Because of the way most computer systems are configured, it is not likely that an e-mail message can be intercepted, prior to its passing through a server, so as to invoke Title I of the ECPA. *See, e.g.*, U.S. v. Moriarty, 962 F. Supp. 217 (D. Mass. 1997) (holding that interception of electronic communications only applies to accessing information while in transmission).

52. *See* 18 U.S.C. § 2701(c) (1998).

53. Larry O. Natt Gantt, II, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J.L. & TECH. 345, 364 (1995). One commentator has differentiated the business use exception from a separate service provider exception. This was done because his analysis focused upon the telephone interception cases and then the application of those cases to the issue of e-mail service providers. For the purposes of this comment, based upon 18 U.S.C. § 2701(c), there is only one exception, the business use exception. *But see* Jarrod J. White, *E-Mail@Work.Com: Employer Monitoring of Employee E-Mail*, 48 ALA. L. REV. 1079,1086–90 (1997).

The consent exception is more straight forward, because it provides that access is allowed when given "with respect to conduct authorized . . . (2) by a user of that service with respect to a communication of or intended for that user."[54] Commentators have summarized this exception as: "The most certain protection against liability under the ECPA exists when express consent has been given by an employee prior to any interception or access of E-mail in electronic storage."[55] One commentator stated that this consent "may be expressly given, and in some cases reasonably implied from the surrounding situation."[56] The basis for analyzing a person's consent to monitoring has often been analogized to the telephone monitoring cases, which normally involve the interception of communications.[57] However, from these cases it is not clear whether consent for the purposes of intercepting a communication must be express to that interception or can be implied.[58] In the voice messaging system case of *Bohach v. City of Reno*, the court found that the consent exception of Title II of the ECPA includes a person's implied consent to the accessing of messages, when it is known by him that messages in the system can be accessed by other parties prior to using the system.[59]

While courts have not clearly developed the basis of the consent exception, the parameters of the "business use" exception may be even more difficult to clarify for the purposes of accessing e-mail under Title II of the ECPA. The exception is stated as "with respect to conduct authorized—(1) by the person or entity providing a wire or electronic communications service."[60] For the purposes of e-mail, § 2701(c)(1) is especially vague because an e-mail service provider can be either the firm providing a user with service, or a firm providing a user access to a service provided by another company. Today e-mail services can be provided to firms by e-mail service providers, providers of telecommunication services generally, or the firm may have its own server. In each of these cases based upon the language of the statute, it is not clear how

54. 18 U.S.C. § 2701(c)(2).

55. *See* White *supra* note 53, at 1083–84; *see also* Anne L. Lehman, *E-Mail in the Workplace: Question of Privacy, Property or Principle?*, 5 COMM. LAW CONSPECTUS 99, 103 (1997) stating: "[I]f a company that supplies e-mail service to its employees is seen as a service provider, simple authorization from the company is required to access the stored messages received and sent by its employees."

56. Sally D. Garr, *Employee Monitoring and Privacy in the Internet Age*, SB53 ALI-ABA 1, 11 (1997) (citing Deal v. Spears, 980 F.2d 1153, 1158 (8th Cir. 1992)).

57. *See id.* at 9; White, *supra* note 53, at 1083–85; Gantt, *supra* note 53, at 356; David Neil King, Note, *Privacy Issues in the Private-Sector Workplace: Protection from Electronic Surveillance and the Emerging "Privacy Gap"*, 67 S. CAL. L. REV. 441, 451–54 (1994).

58. *See Spears*, 980 F.2d 1153; *Watkins*, 704 F.2d 577.

59. Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996).

60. 18 U.S.C. § 2701(c)(1) (1998).

the ECPA's exception applies. If the exception can be applied, it essentially gives the "provider" unlimited access to the contents of stored communications.[61] One commentator has summarized § 2701(c)(1)'s exception as:

> Courts have interpreted this provision [Title I's similar "business use" exception] to exclude from the law's prohibitions interceptions by an employer of employee communications, provided such interceptions have occurred in the ordinary course of the employer's business. Though none of these cases has involved e-mail, their analysis of the business exception can be applied to e-mail.[62]

Since that was written, there still have not been any workplace e-mail cases addressing this issue; however, the *Bohach* case did address the provider exemption issue.[63] Additionally, the court in *Andersen Consulting LLP v. UOP*, addressed an aspect of the provider exception.[64] While these cases do not definitively answer the question of who is a provider for the purposes of workplace e-mail, they shed light on how courts are inclined to interpret 18 U.S.C. § 2701(c)(1).

In *Bohach*, the court found that the City of Reno, for the purposes of the ECPA, was a provider of the communications service, a computerized internal voice messaging system and was therefore "free to access the stored messages as it pleased."[65] The court's reasoning for finding no ECPA access violation, was that "§ 2701(c)(1) allows service providers to do as they wish when it comes to accessing communications in electronic storage."[66] This statement is the extent of the court's consideration about whether the city was a service provider of the communications services for the purpose of an ECPA access violation.[67] Reaching its final conclusion that the city would not violate the ECPA in accessing the voice messaging communications of two police officers under investigation, the court stated: "Because the City is the provider of the 'service,' neither it nor its employees can be liable under § 2701."[68]

---

61. *See* Ruel Torres Hernandez, *ECPA and Online Computer Privacy*, 41 FED. COMM. L.J. 17, 39–41 (1988); *see also* Pedrow, *supra* note 26, at 37.

62. Pedrow, *supra* note 26, at 37.

63. *See Bohach*, 932 F. Supp. at 1235–36.

64. Andersen Consulting LLP v. UOP, 991 F. Supp 1041, 1042 (N.D. Ill. 1998).

65. *Bohach*, 932 F. Supp. at 1237.

66. *Id.* at 1236.

67. *See* discussion *infra* pp. 14–15 (discussing that once there is a finding that a firm is a service provider of the communications service, under the exception of § 2701(c)(1) the firm is at liberty to access all stored communications of that service).

68. *Bohach*, 932 F. Supp. at 1236.

In *Andersen*, the court found that the ECPA had not been violated by UOP[69] when it disclosed e-mail messages from Andersen employees to the Wall Street Journal. The Andersen employees had been working for UOP as contractors, and had been using UOP's e-mail system in the course of their contract work for UOP.[70] UOP, unhappy with Andersen's work, released the Andersen employees' e-mail messages, stored on the UOP computer system, to the Wall Street Journal for their publication in a story about the breach of contract action brought by UOP against Andersen.[71] Andersen filed a separate action against UOP alleging a violation of the ECPA through the release of the e-mail messages.[72] Andersen argued that as a contractor they were allowed to access UOP's system causing UOP to be a public service provider, therefore UOP's accessing and release of the e-mail messages was in violation of the ECPA pursuant to 18 U.S.C. § 2702.[73] The court in dismissing the action, found that UOP was not a public service provider under 18 U.S.C. § 2702(a)(1), but only provided services to its employees which included the Andersen employees while they were contracting with UOP.[74]

The *Andersen* case was brought under the theory that UOP was a public service provider of e-mail services for the purpose of the ECPA.[75] The significance of the *Andersen* case is the court's statement that UOP was a service provider. While the case does not provide an analysis of Andersen's claim under § 2701's exceptions, the outcome of the case assumes that because Andersen was a service provider, but not a provider for the purposes of § 2702, § 2701 was not violated by UOP's release of the Andersen employee's e-mail messages to the Wall Street Journal. This result is consistent with the court's statement in *Bohach* that "[b]ecause the City is the provider of the 'service,' neither it nor its employees can be liable under § 2701."[76]

---

69. UOP is "a joint venture of Allied Signal Inc. and Union Carbide Corp. . . .", Elizabeth MacDonald, *Workplace: E-Mail Trail Could Haunt Consultant in Court*, WALL ST. J., June 19, 1997, at B1.

70. *See Andersen*, 991 F. Supp. at 1041; *see also* MacDonald, *supra* note 69, at B1 (the story that caused the allegation of the ECPA violations).

71. *See Andersen*, 991 F. Supp. at 1041. It is not difficult to understand Andersen's outrage at UOP for the disclosure of the e-mail messages for publication in the newspaper. Among other things contained in the messages, "consultants sent disparaging messages about each other. 'It's horrible,' one Andersen consultant wrote about a colleague. 'He has his hot, sweaty face just inches from yours, like some kind of putrid pumpkin.' " MacDonald, *supra* note 69, at B1.

72. *See Andersen*, 991 F. Supp. at 1041, 1042.

73. *See id.*

74. *See id.*

75. *See id.*

76. *Bohach*, 932 F. Supp. at 1236.

Older cases brought under the ECPA, usually involving the interception of telephone calls, raised distinctions that the "business use" exception of the ECPA applied only when "the employer had a legitimate business purpose to justify the interception of the employee's communication."[77] However, it is not clear that such a distinction must be made for e-mail communications accessed under § 2701. Under § 2701, the employer would only have to show that the firm is a provider. This showing would require a firm to show how e-mail services are provided to the e-mail users of the firm.

Congress's intent as to who is to be considered a service provider is not clear.[78] Whether Congress only intended § 2701's exceptions to apply to public, commercial providers, such as CompuServe, when they provide e-mail services to other companies if it was to apply to firms when they provide e-mail services to their employees through their own servers remains unclear.[79] Section 2702 clearly states that public service providers have a "business use" exception to access e-mail messages when they provide e-mail services to the public at large.[80] However, whether e-mail services provided by a firm to users, gives the firm an exception to access a user's e-mail messages is not clear.[81] The recent cases of *Bohach* and *Andersen* demonstrate that courts are inclined to interpret this gray area to mean that for the purposes of § 2701, firms providing e-mail services to their employees are exempted from § 2701's prohibitions against accessing stored e-mail communications under § 2701(c)'s exceptions.[82]

B. *Privacy for Consumers and Workers Act*

Because the ECPA has not been directly applied to the issue of accessing workplace e-mail communications, and also because the current

77. Kevin J. Baum, Comment, *E-mail in the Workplace and the Right of Privacy*, 42 VILL. L. REV. 1011, 1026 (1997).

78. *See* White, *supra* note 53, at 1089; David R. Johnson, *Privacy: Good Sysops Should Build Good Fences*, (visited Apr. 13, 1998) <http://www.eff.org/pub/Privacy/good_fences_johnson.article>, "Those who provide electronic communications services—a category that will increasingly include most large companies . . . ."

79. *See* White, *supra* note 53, at 1089.

80. *See* 18 U.S.C. § 2702 (1998).

81. "Depending upon how the term 'entity providing an electronic communications service' is construed, employers who provide the electronic communications service that their employees use, may have unfettered right to access stored employee communications. The case law in this area is very sparse and so unclear that even legal commentators are in dispute." Garr, *supra* note 56, at 9.

82. *See* discussion *infra* Part II.D.3.a (discussing the unreported case of Shoars v. Epson America, Inc., a case preceding Bohach, where the court supported this interpretation of § 2701(c)(1)'s exceptions).

ECPA case law renders an interpretation of the Act that provides minimal restraint on a firm's accessing of users' e-mail communications and a minimal recognition of users' privacy interest in e-mail communications, questions remain about how, when and for what purposes workplace e-mail communications may and should be accessed. These issues have in part spawned additional congressional efforts to address the issue of electronic workplace monitoring of employees. The most pronounced of these was the Privacy for Consumers and Workers Act (PCWA) originally introduced into Congress in 1991.[83] Similar legislation was introduced in 1992 and 1993.[84] None of this legislation has been enacted into law.

The legislation that has thus far been introduced has followed a consistent pattern and is illustrative to show how Congress has framed solutions to some of the problems posed by the ECPA and more generally to the issue of employee electronic monitoring. The approach of the PCWA is to look generally at the issue of employee electronic monitoring of which e-mail monitoring is but one component. The introduction of H.R. 1218, the first PCWA legislation, states the purpose of the legislation is "to protect employees from burdensome secret electronic monitoring in the workplace by providing employees with notice when they are being monitored electronically while performing their jobs."[85] Workplace e-mail, one area where electronic monitoring occurs, was discussed as needing protection because: "[e]lectronic mail interception exposes employee's electronic mail messages to their employer's scrutiny. As computers are increasingly linked together locally, nationally, and internationally, employers and others can more easily penetrate and abuse corporate computer systems and information."[86]

One commentator summarized the provisions of the PCWA, in the context of e-mail monitoring, as follows:

> [T]he law would allow employers to monitor employee's e-mail and, to some extent, use the information collected against employees. Before doing so, however, employers would be required to inform employees that their communications are subject to monitoring and also to inform them of the form and scope of the monitoring and use to be made of the data collected.[87]

83. *See* H.R. REP. NO. 102-1024, at 1 (1992), *reprinted in* 1992 WL 316386.
84. *See* S. 984, 103d Cong. (1993).
85. H.R. REP. NO. 102-1024, at 8 (1992), *reprinted in* 1992 WL 316386.
86. H.R. REP. NO. 102-1024, at 13 (1992), *reprinted in* 1992 WL 316386.
87. Pedrow, *supra* note 26, at 38.

The thrust of the PCWA is to provide a structure for employer electronic monitoring to take place over some employees while providing those employees with procedural safeguards in which the monitoring must take place. Because the PCWA is designed to cover all aspects of electronic monitoring, some issues discrete to e-mail, but not raised by other forms of electronic monitoring are not thoroughly addressed.[88] One commentator discussing the PCWA has stated:

> [The PCWA] is certainly a major step toward adequate privacy protection for the employee in the private-sector workplace . . . . However, the passage of the PCWA would still leave employees subject to offensive non-electronic monitoring, and fails to protect the employee against egregious privacy violations that meet the notice requirements of the Act.[89]

Some commentators have criticized the PCWA for being too pro-employee while others have stated that the PCWA does not go far enough in protecting employee interests.[90] Still others have praised the PCWA for even attempting to address the issue. The PCWA, however, is not law. It is a recognition by some members of Congress that there is a problem regarding employee privacy. More so, it is an indication of the way Congress may frame the issue of employee monitoring in the future and of the type of solution that Congress sees for the problems raised by employee monitoring. There are better ways to frame the issue of employer monitoring of e-mail and better solutions to the problem than what have been proposed in the PCWA.

C. *Electronic Mail Cases*

There have been few reported cases addressing the monitoring of workplace e-mail.[91] The only reported cases to address the issue are

88. *See, e.g.*, Laurie Thomas Lee, *Watch Your E-mail! Employee E-mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop"*, 28 J. MARSHALL L. REV. 139, 167–68 (1994) (noting that the proposed law would not address the issue of how the PCWA's protections and policies would be affected by the ECPA); *see also* Araneo, *supra* note 12, at 356. The author notes that e-mail should not be compared directly with telephone or postal communications in addressing employer monitoring because "[e]-mail has its own identity and character, and ultimately it brings to the table new problems of employee privacy and employer monitoring." *Id.*

89. King, *supra* note 57, at 473.

90. *Compare id. with* Gantt, *supra* note 53, at 410.

91. There have been several cases where e-mail has been a factor in the case, but these cases have not dealt with the central issue of who does, can and should have access to user's e-mail messages. *See* Lian v. Sedgwick James of New York, Inc., No. 96 Civ. 5129(DC), 1998 WL 30284, at *1 (S.D. N.Y. Jan 28, 1998) (employment defamation suit brought by an employee based upon an e-mail message sent by the employer to other employees about the terms of the former employee's termination); Owens v. Morgan Stanley & Co., No. 96 CIV.

Restuccia v. Burk Technology, and *Smyth v. Pillsbury Company*.[92] There are several other unreported cases that address this issue, all of which arose in California state courts.[93] All of the cases, reported and unreported, to address e-mail monitoring in the workplace have been based upon state law claims and none of them have raised claims pursuant to the ECPA. Some of these cases have raised issues under state statutes which mirror the ECPA, but it is not clear why ECPA claims were not raised in any of these cases.

Looking at these cases is instructive because they demonstrate the type of recognition that state courts have given to e-mail users' claims in response to the accessing of their e-mail communications. These cases also demonstrate how e-mail users have framed their claims and the lack of success that most have faced in raising a claim against improper access of their e-mail communications. Most importantly, these cases demonstrate that state law may provide some recognition, at least more recognition than the ECPA currently provides, that e-mail users have a protected privacy interest in their e-mail communications. Nevertheless in most cases, this recognition is still tenuous.

1. Restuccia v. Burk Technology

Restuccia and LoRoe were employed at Burk Technology where they used the office e-mail system.[94] Mr. Burk, the president of Burk,

---

9747(DLC), 1997 WL 793004, at *1 (S.D. N.Y. Dec. 24, 1997) (employment discrimination claim by an employee stemming from racist e-mail messages.); Donley v. Ameritech Services, Inc., No. 92-72236, 1992 WL 678509, at *1 (E.D. Mich. Nov. 16, 1992) (wrongful termination suit brought by an employee for sending an inappropriate e-mail message about a client).

92. Restuccia v. Burk Technology, Inc. 5 Mass L. Rptr. No. 31, 712 (November 4, 1996); Smyth v. Pillsbury Company, 914 F. Supp. 97 (E.D. Penn 1996).

93. Bourke v. Nissan Motor, Co., No. YC 003979 (Cal. Super. Ct. filed Feb, 1, 1991) (a copy of the appellate decision of July 26, 1993 can be found online at <http:www.law.seattleu.edu/chonm/Cases/bourke.html.>, (visited Apr. 13, 1998); the appellate court affirmed the trial court's decision); Flanagan v. Epson America, Inc., No. BC 007036 (Cal. Super. Ct. filed July 31, 1990); Shoars v. Epson, America, Inc., No. SWC 112749 (Cal. Super. Ct. filed Mar. 26, 1990). While it has not been reported, there was a civil suit filed in the case of Eugene Wang leaving Borland for Symantech by Wang against his former firm, Borland, for Borland's review of his e-mail messages immediately after he announced his resignation from Borland to join Symantech. *See* John Burgess, *Criminal Probe Launched Over Trade Secrets: Software Firms Charges Executive Took Information*, WASH. POST, Sept. 8, 1992, at E1; John Thackray, *The E-mail is Deadlier . . .—Electronic Mail Has Added a Bizarre New Dimension to US Office Politics*, THE OBSERVER, May 1, 1994, at 8. A criminal case was brought against Wang and Borland for misappropriation of trade secrets. The criminal case raised a unique issue of conflict of interest because Borland provided financial assistance to the district attorney's office in investigating the computer system of Borland. *See* People v. Eubanks, 927 P.2d 310, 312–14 (Cal. 1997).

94. *See Restuccia*, 5 Mass L. Rptr. No. 31, at 712.

fired Restuccia and LoRoe after accessing the company's e-mail system and reviewing their e-mail messages discovering that they referred to him by various nicknames and knew about his extra-marital affair. [95] Mr. Burk reviewed e-mail messages stored in the company system for eight hours after a staff meeting where LoRoe had protested new office policies and another employee told Burk about LoRoe's e-mail use.[96] Mr. Burk stated that he fired LoRoe and Restuccia for their excessive e-mail use—not the content of their messages.[97]

To use the Burk e-mail system, a user had to log on with a personally selected password.[98] The firm had no policy about e-mail use other than that "excessive chatting" should not take place.[99] Restuccia and LoRoe were not told and did not know that their supervisors could gain access to their e-mail messages.[100] After their termination, they brought a suit against Burk Technology for wrongful termination, invasion of privacy, unlawful interception of wire communications, intentional and negligent infliction of emotional distress, loss of consortium and interference with contractual relations.[101] Burk moved for summary judgment on all claims, which was granted except for the claims of wrongful termination, invasion of privacy, negligent infliction of emotional distress and loss of consortium.[102]

Restuccia and LoRoe failed on their claim of unlawful interception of wire communication, brought pursuant to the Massachusetts statute G.L.C. 272, § 99.[103] This statute prohibits the "secret hearing or secret recording of wire communications by means of an intercepting device."[104] The statute also provided for what is called a "business use exception" to the interception prohibitions.[105] The court read the statute to exempt the actions of Burk in accessing the stored e-mail messages.[106]

The court found that Restuccia and LoRoe had raised an issue which presented a question of fact as to whether Burk's review of their e-mail messages was an invasion of privacy and grounds for wrongful termination.[107] The court found that there was a question of fact as to whether

95. *See id.*
96. *See id.*
97. *See id.*
98. *See id.*
99. *See id.*
100. *See id.*
101. *See id.*
102. *See id.*
103. *See id.* at 713.
104. *See id.*
105. *See id.*
106. *See id.*; *see* discussion *supra* p. 11 (about the ECPA's "business use" exception).
107. *See id.* at 714.

Restuccia and LoRoe had a reasonable expectation of privacy for their e-mail messages.[108] The court also found that there was a material question of fact as to whether the firing of Restuccia and LoRoe, who were at-will employees, violated the public policy of the privacy statute.[109]

2. Smyth v. Pillsbury Company

Smyth provides an interesting comparison to *Restuccia*.[110] Both cases involve similar fact scenarios and similar claims by the employee. However, Restuccia's claims survived a pre-trial motion, while Smyth's claims did not. Smyth was an employee of the Pillsbury Company.[111] He sent an e-mail from home to his supervisor concerning sales management containing the phrase "kill the backstabbing bastards" and "referred to the planned Holiday party [at Pillsbury] as the 'Jim Jones Koolaid affair.' "[112] Employees at Pillsbury were informed that their e-mail messages would remain confidential and privileged and that e-mail messages could not be used against an employee "as grounds for termination or reprimand."[113] Smyth's stored e-mail was accessed by his superiors at Pillsbury and he was terminated for "transmitting . . . inappropriate and unprofessional comments."[114]

Smyth was an at-will employee and brought a claim in federal district court against Pillsbury for wrongful termination.[115] The court, in granting a motion to dismiss the claim, found that Smyth had no cause of action, because Pennsylvania is an at-will jurisdiction and Smyth's claim did not fit into one of the recognized public policy exceptions to the rule that an at-will employee may be discharged for any reason.[116] Smyth argued, similar to Restuccia, that his discharge was against a claimed public policy of the common law doctrine of invasion of privacy.[117] The court found this unpersuasive as the public policy exception was narrowly limited to three exceptions: serving on jury duty, denying employment to a person with a prior conviction and termination for reporting nuclear regulatory violations.[118]

---

108. *See id.*
109. *See id.*
110. *Compare Restuccia*, 5 Mass L. Rptr. No. 31, at 712–14, *with Smyth*, 914 F. Supp. at 98–100.
111. *See Smyth*, 914 F. Supp. at 98.
112. *Id.* at 98 n.1.
113. *Id.* at 98.
114. *Id.* at 99.
115. *See id.* at 98.
116. *See id.* at 99.
117. *See id.*; *Restuccia*, 5 Mass L. Rptr. No. 31, at 714.
118. *See Smyth*, 914 F. Supp. at 99.

The court then continued in dicta[119] to consider the merits of a claim under the tort of invasion of privacy if Smyth had brought such a claim.[120] While this discussion arose concerning the public policy exemption to the at-will employee doctrine, the court's analysis shifted to focus on the merits of a claim by Smyth for invasion of privacy.[121]

Smyth argued that he had a reasonable expectation of privacy based upon the prior Pennsylvania case of *Borse v. Piece Goods Shop*.[122] *Borse* involved an employee's claim that termination for refusal to take a urinalysis test was an invasion of privacy, violated public policy and constituted an exception to the at-will doctrine.[123] The court in *Smyth* compared the situation of a urinalysis test to that of Smyth's e-mail and found that Smyth, despite Pillsbury's statements to the contrary, did not have an expectation of privacy in his e-mail communications and even if he did, that expectation was lost once he sent the e-mail messages over the company's system.[124] The court also found that a reasonable person would not consider Pillsbury's interception of the e-mail messages a highly offensive invasion of privacy.[125]

3. California State Cases

There have been several California cases to address the issue of workplace e-mail monitoring.[126] These cases, all unpublished, presented similar fact patterns and were based upon similar causes of action. Although unreported, these cases have been extensively analyzed.[127] These

---

119. *See* Kent Greenawalt, *Reflections on Holding and Dictum*, 39 J. LEGAL EDUC. 431 (1989).

120. *See Smyth*, 914 F. Supp. at 100–01.

121. *See id*.

122. *See id.* at 100 (citing Borse v. Piece Goods Shop, Inc., 963 F.2d 611 (3d Cir. 1992)).

123. *Borse*, 963 F.2d at 613. The Third Circuit Court of Appeals, in a lengthy analysis of the Pennsylvania at-will employment doctrine, predicted that the state supreme court would find that termination for a refusal to submit to a urinalysis would violate public policy and be an exception to the at-will employment doctrine. However, the court was unclear whether Borse had properly stated such a claim, so they vacated the district court's order dismissing the complaint and remanded the case with instructions for Borse to amend her complaint. *Id.* at 626.

124. *See Smyth*, 914 F. Supp. at 101.

125. *See id.*

126. Bourke v. Nissan Motor, Co., No. YC 003979 (Cal. Super. Ct. filed Feb 1, 1991) (a copy of the appellate decision of July 26, 1993 can be found online at <http:www.law.seattleu.edu/chonm/Cases/bourke.html.> (visited Apr. 13, 1998); the appellate court affirmed the trial court's decision); Flanagan v. Epson America, Inc., No. BC 007036 (Cal. Super. Ct. filed July 31, 1990); Shoars v. Epson, America, Inc., No. SWC 112749 (Cal. Super. Ct. filed Mar. 26, 1990).

127. *See, e.g.*, Rochelle B. Ecker, Comment, *To Catch a Thief: The Private Employer's Guide to Getting and Keeping an Honest Employee*, 63 UMKC L. REV. 251, 269–70

cases are also significant, because they provide further illustrations of how plaintiffs have framed their causes of actions, again underscoring the problem of e-mail privacy and the gray areas of the ECPA. These cases were brought in California state courts, which are known for their innovative approaches to the law.[128] In addition, unlike other states or the federal Constitution, California also has a state constitutional provision which "establishes privacy as a fundamental right of citizens in this state."[129]

a. Shoars v. Epson, Inc. and Flanagan v. Epson, Inc.

Shoars and *Flanagan* arose out of the same set of facts.[130] Shoars was an Office Systems Programmer Analyst in the Information Resources Department at Epson America, Inc..[131] In 1990, she discovered that her direct supervisor had "systematically printed up and read all of the E-mail that was entering and leaving Epson's place of business . . . ."[132] Shoars "had been informing Epson employees that their e-mail transmissions were confidential. She also believed that no one in Epson had given her supervisor consent to read the transmissions."[133] Shoars requested a private e-mail account number from Epson's main systems administrator, which her supervisor could not access, a request which her supervisor intercepted. Her supervisor then terminated her for insubordination.

Shoars brought a claim under California Penal Code § 631, a wiretap law similar to the ECPA, claiming that Epson had violated her right to privacy in the workplace with a wiretap.[134] Shoars' claim was dis-

(discussing Shoars v. Epson America, Inc.); Lee, *supra* note 88, at 142 (discussing Shoars v. Epson America, Inc.); Gantt, *supra* note 53, at 359–60 (discussing Flanagan v. Epson America, Inc.); Winters, *supra* note 21, at 221–31 (discussing Shoars v. Epson America, Inc.); Morris, *supra* note 42, at 341–343 (discussing Flanagan v. Epson America, Inc., Shoars v. Epson America, Inc., and Bourke v. Nissan Motor Co.); and White, *supra* note 53, at 1096–97 (discussing Flanagan v. Epson America, Inc., Shoars v. Epson America, Inc., and Bourke v. Nissan Motor Co.).

128. *See* Julia Turner Baumhart, *The Employer's Right to Read Employee E-mail: Protecting Property or Personal Prying?*, 8 LAB. LAW. 923, 944 (1992); *see also* Victoria Slind-Flor, *What Is E-mail, Exactly?*, NAT'L L.J., Nov. 25, 1991, at 3.

129. In the case of Hill v. National Collegiate Athletic Association, the California Supreme Court stated that this right extends to private-sector employees. Hill v. National Collegiate Athletic Association, 865 P.2d 633, 641 (Cal. 1994); *see also* Barker, *supra* note 20, at 1143; Baumhart, *supra* note 128, at 944.

130. *See* Morris, *supra* note 42, at 341.

131. *See* Winters, *supra* note 21, at 223.

132. *Id.*

133. *Id.*

134. *Id.* at 224; *see also*, Charles Piller, *Bosses with X-Ray Eyes*, MACWORLD, July 1993, at 122, "[Shoars's] attorney, Noel Shipman, Claims that by reading employee E-mail

missed. One commentator examining the case, summarized the court's reasoning for finding that there was no violation of the California state statute stating:

> First, the court concluded that it was not clear plaintiff [Shoars] had an expectation of privacy. Without such an expectation, there could be no invasion of that privacy through wiretapping. The superior court did not elaborate on this statement . . . . Second, the court assumed, and found *arguendo*, that even if plaintiff had an expectation of privacy, E-mail was not covered by section 631 . . . . Third, the court in Shoars held that section 631 did not cover interception of E-mail communications despite the broad statement of intent offered by the California legislature in section 630 of the California Penal Code.[135]

This commentator went on to note that the superior court in *Shoars* referred to the ECPA for their interpretation of § 631, and following the statements of another commentator on the purpose of the ECPA concluded that:

> "under 2701 [of the ECPA], although it may be illegal for others to gain access without authorization or to exceed authorized access to a system [under the ECPA], 'the person or entity providing a wire or electronic communications service' is not liable for any offenses regarding stored communications, i.e., voice mail, E-mail, or other recorded communications."[136]

In other words, there simply is no ECPA violation if " 'the person or entity providing a wire or electronic communications service' intentionally examines everything on the [electronic mail] system."[137]

Flanagan was a class action brought by the employees whose e-mail had been read by Shoars's supervisor.[138] The *Flanagan* case was brought under the same claims as Shoars's action.[139] Likewise, the case was dismissed by the court. "The *Flanagan* court refused to extend California's right to privacy to employee E-mail, suggesting that such a determination should be left to the legislature."[140]

---

messages, Epson violated both the state constitution's privacy provision as well as a California eavesdropping statute."

135. *See* Winters, *supra* note 21, at 226–27.

136. *Id.* at 227 (citing Hernandez, *supra* note 61, at 39).

137. Winters, *supra* note 21, at 227.

138. *See* Morris, *supra* note 42, at 341; Gantt, *supra* note 53, at 397.

139. *See* Morris, *supra* note 42, at 341.

140. White, *supra* note 53 , at 1097; *see also* Morris, *supra* note 42, at 341–42.

b. Bourke v. Nissan Motor Corp.

Another employee e-mail monitoring case arose when Nissan Motors Corporation reviewed the e-mail communications of two Nissan employees, Bourke and Hall, who were Information Systems Specialists for Nissan Motors.[141] As the appellate court stated, "[p]laintiffs were essentially customer service representatives for users of the computer system."[142] Bourke and Hall were involved in an e-mail demonstration where some of their e-mail messages were used to demonstrate the e-mail system at which time another Nissan employee read their messages, reporting their content to a supervisor.[143] The messages were " 'of a personal, sexual, nature and not business related.' "[144]

Bourke and Hall brought an action against Nissan based on Nissan's violation of California's constitutional right to privacy, Nissan's violation of the California wiretap statute, specifically §§ 631 and 632, and wrongful discharge in violation of public policy.[145] The appellate court affirmed the trial court's order of summary judgment for Nissan.[146] In so doing, the appellate court concluded that there was no constitutional violation, because the plaintiffs knew that their e-mail could be read. They had signed a Nissan company agreement stating that their e-mail use was to be for business use only.[147] The plaintiffs also had no expectation of privacy, because other employees had previously told them that the company reviewed employee e-mail.[148] Bourke and Hall argued that they had an expectation of privacy, because they used a password to access their messages.[149] The court stated that the password issue might raise a question of fact, but "the question presented to us is whether their expectations of privacy were objectively reasonable as a matter of law."[150]

On the issue of §§ 631 and 632, the facts of *Bourke* differed from those of *Shoars* and *Flanagan*, because in *Bourke*, the e-mail messages had not been "intercepted" but clearly accessed from storage. In *Bourke*, there was less of an issue about an "interception," because the facts make it clear that the communications were not intercepted but ac-

141. Bourke v. Nissan Motor Co., No. B068705, at *1 (Cal. Ct. App. July 26, 1993) (visited Apr. 13, 1998) <http://www.law.seattleu.edu/chonm/Cases/bourke.html>.

142. *Id.*

143. *See id.*

144. *Id.*

145. *See id.* at *3–4.

146. *See id.* at *1.

147. *See id.* at *3.

148. *See id.*

149. *See id.*

150. *Id.* at *3.

cessed, and §§ 631 and 632 clearly state their prohibition is against interception.[151] Because there was no invasion of privacy by Nissan in reading the e-mail messages, the court found that there could be no discharge in violation of public policy exception applied to the termination of Bourke and Hall, who were at-will employees.[152]

IV. SOLUTIONS

A. *Common Law Tort Claims*

Restuccia v. Burk is the only workplace e-mail case to have survived a pre-trial attack of the e-mail user's claims. This case was brought pursuant to Massachusetts statutory law, part of which is a codification of the common law tort of invasion of privacy.[153] *Restuccia*'s survival was due to the type of claims upon which the case was brought, as compared to *Smyth*, and the way in which the trial court interpreted the application of the elements for the invasion of privacy claim under Massachusetts law. *Restuccia* shows that an e-mail user can raise a successful claim to e-mail monitoring. While the strength of the claim will be dependent upon the facts of the case, *Restuccia* demonstrates that raising a triable claim is possible, *i.e.*, the invasion of privacy tort is the e-mail user's most likely avenue for successful redress.[154]

To prevail under the invasion of privacy tort, the e-mail user must show that a reasonable expectation of privacy exists, that this expectation was reasonably held, and that the operator of the e-mail system did not have a legitimate purpose for the intrusion.[155] Being able to prove these facts may not be possible in all cases. *Smyth* and *Shoars* are examples of cases not surviving pre-trial attack.[156] The court in *Smyth* stated that Smyth did not have a reasonable expectation of privacy nor would a reasonable person "consider the defendant's interception of these communications to be a substantial and highly offensive invasion of his privacy."[157] In *Shoars*, the court just assumed that none of the

151. *See id.* at *4.

152. *See id.*

153. *Compare Restuccia*, 5 Mass L. Rptr. No. 31, at 714, *with* RESTATEMENT (SECOND) OF TORTS § 652B (1977); *see* discussion *supra* Part I.B.2.

154. "For the typical private sector employee, the only general source of legal protection for unjustified employer intrusion is the common law." Pauline T. Kim, *Privacy Rights, Public Policy, and the Employment Relationship*, 57 OHIO ST. L.J. 671, 675 (1996).

155. *See* RESTATEMENT (SECOND) OF TORTS § 652B (1977).

156. *See Smyth*, 914 F. Supp. at 98; Winters, *supra* note 21, at 226.

157. *Smyth*, 914 F. Supp. at 101.

system's users had a reasonable expectation of privacy, but did not provide any justification for this assumption.[158]

The court's reasoning in *Smyth* is suspect for two reasons. First the court notes, at the beginning of the decision, that Pillsbury had "repeatedly assured its employees, including [Smyth], that all e-mail communications would remain confidential and privileged," and also "that e-mail communications could not be intercepted and used by [Pillsbury] against its employees as grounds for termination or reprimand."[159] The court rationalized, that despite these statements by Pillsbury, Smyth should still not have had any expectation of privacy.[160] The court suggests this is because the e-mail system was "apparently utilized by the entire company."[161] The suggestion is that because the entire company uses the e-mail system, Smyth could not have thought that his communications would be confidential, or, as the company policy also stated, privileged.[162] Black's Law Dictionary defines confidential as "intended to be held in confidence or kept secret," and privileged as "possessing or enjoying a privileged."[163] Pillsbury's policy clearly states to the user of the e-mail system that the company will not intercept the user's e-mail.[164]

Additionally, the company policy stated that e-mail will not be the basis for a user's termination.[165] The court viewed Pillsbury's right to know about Smyth's statements as outweighing any interest Smyth had.[166] Again, the court did not pay attention to the company's policy and what they had told Smyth, but placed greater reliance upon their own view of how the interests should be balanced. As one commentator has noted, "courts have been reluctant to protect employee's privacy interests because their interests often clash with the employer's interest in monitoring and efficiently managing the work force."[167]

The second factor that the court does not account for is that most people believe that their e-mail communications are protected in some way from the view of other people.[168] Despite numerous sources that say

158. *See* Winters, *supra* note 21, at 226.
159. *Smyth*, 914 F. Supp. at 98.
160. *See id.* at 101
161. *Id.*
162. *See id.*
163. BLACK'S LAW DICTIONARY 297, 1198 (6th ed. 1990).
164. *See Smyth*, 914 F. Supp. at 98.
165. *See id.*
166. *See id.* at 101.
167. Gantt, *supra* note 53, at 403–04.
168. "Employees . . . tend to assume that their E-mail files have the same degree of privacy as perhaps their desks, their briefcases, or their purses. When an issue arises over management accessing someone's E-mail files, the employee is the one who feels violated."

e-mail is like a postcard and one should not transmit anything via e-mail that one would not want read aloud to a group, people constantly send all sorts of personal messages over company e-mail systems.[169] This shows that people in fact have an expectation that their e-mail communications are private and that most would find it "highly offensive" to have their communications read by someone other than an intended recipient.[170] The court in deciding *Smyth*, was not considering the way e-mail is used on a daily basis.[171] Had Smyth filed a claim based upon an invasion of privacy and not wrongful termination he may have been more successful.[172] Also, perhaps if the *Smyth* case had been tried in a Pennsylvania state court, Smyth might have had a better outcome in a court in a position to make precedent setting state law.[173]

In spite of *Smyth* and the California cases, and as demonstrated by *Restuccia*, the common law invasion of privacy tort is the only available basis for persons seeking redress for unwarranted monitoring of e-mail.[174] As of yet, the ECPA remains largely untested as a remedy for e-mail users to base a claim for improper access to a stored communication. The

---

Stop Agonizing—Implement an E-mail Privacy Policy, ELECTRONIC MESSAGING NEWS, Nov. 24, 1993; *see* Soden, *supra* note 4, at 1.

169. "Many employees consider e-mail a modern day water cooler for gossip and discussion." Richard J. Loftus et al., *Cutting Edge Tech Can be Double-edged Sword*, NAT'L L.J., Nov. 3, 1997, at B11.

170. Alan Westin in his recent examination of privacy in the workplace concluded that most people do not object to an employer using electronic monitoring when the employee is communicating directly with customers or for some direct business purpose. However, outside of this narrow area of monitoring he states, "[w]hen some pollsters have asked the public whether it is all right for employers to 'listen-in on the telephone calls of their employees,' the reactions are thoroughly predictable—the public says no." Alan F. Westin, *Privacy in the Workplace: How Well Does American Law Reflect American Values?*, 72 CHI.-KENT L. REV. 271, 278 (1996). "One recent, national public-opinion survey found that eighty-one percent of Americans think employers lack the right to monitor personal telephone calls, ..." King *supra* note 57, at 441–42. "Under most circumstances, employees have a reasonable expectation of privacy regarding the contents of their desks, interoffice memos, telephone conversations, and electronic and voice mail messages." Bob Lewis, *IS Survival Guide: The Feds are Going too Far with Security; You are Violating Privacy?*, INFOWORLD, Oct. 14, 1996, at 64.

171. *See*, Mary Curtis, *A Love-Hate-Relationship: Surf Warning Your Employer Has a Legal Right to Monitor Your Computer Activity at the Office*, L.A. TIMES, January 19, 1998.

172. *But see* Garr, *supra* note 56, at 12 (the commentator suggests that the main problem with Smyth's case was the appalling and highly offensive nature of his statements in the e-mail communications).

173. Federal courts do not have the ability to establish state law precedent, *see, e.g.*, Lehman, *supra* note 55, at 111.

174. "Because state statutes and constitutions determine the common law right to privacy, there are no real standards or guidelines that employers and employees can use when determining the legal limits of their rights. There is, however, still a remedy to the wrong." Lois R. Witt, *Terminally Nosy: Are Employers Free to Access Our Electronic Mail?*, 96 DICK. L. REV. 545, 569 (1992).

ECPA cases that have emerged, *Bohach* and *Andersen*, have established that courts are likely to read § 2701(c)'s exception broadly to allow a firm that provides e-mail service to have unlimited access to communications stored on the server.[175] However, the ECPA is still untested on this issue and a different court could provide a different interpretation to § 2701(c)(1).[176] *Restuccia* and the California cases also show that state courts may be unwilling to extend state statutes similar to the ECPA to e-mail users' claims without some additional legislative clarification on the scope of the statute.[177] The invasion of privacy claim of *Restuccia* is the only claim for which a court has suggested that e-mail users have a protected privacy interest in their workplace e-mail communications.

B. *Limiting Workplace E-Mail Privacy*

Users have some type of a privacy interest in their e-mail communications. However, most companies providing e-mail services in conjunction with a user's employment will also state that this right is severely limited by the legitimate business interests of the firm to monitor the e-mail system to ensure that it is used for business purposes and will not cause the firm liability.[178] These firms point to the several grounds on which such liability could develop: e-mail use has been the basis of several recent discrimination and harassment suits by employees or former employees because of messages sent on a firm's e-mail system;[179] e-mail messages provide users with heightened capabilities to misappropriate trade secrets;[180] e-mailed information may cause a loss of trademark protection;[181] and e-mail messages may be introduced as evi-

175. "[T]he City, as the system provider, was free to access the stored messages as it pleased." *Bohach*, 932 F. Supp. at 1237; *see also* Thomas R. Greenberg, *E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 AM. U. L. REV. 219, 249 (1994).

176. *See* Garr, *supra* note 56, at 12; Gantt, *supra* note 53, at 373–74; Susan Ellen Bindler, *Peek and Spy: A Proposal for Federal Regulation of Electronic Monitoring in the Workplace*, 70 WASH. U. L.Q. 853, 871 (1992).

177. *See Restuccia*, 5 Mass L. Rptr. No. 31, at 713; Winters, *supra* note 21, at 227.

178. *See* Soden, *supra* note 4, at 1.

179. *See, e.g.*, *Owens*, 1997 WL 793004, at *1 (employment discrimination claim by an employee stemming from racist e-mail messages.); *Donley*, 1992 WL 678509, at *1 (wrongful termination suit brought by an employee for sending an inappropriate e-mail message about a client).

180. "Take the example of the company that had employees who used company e-mail for six months to start their own competing company. They encrypted e-mail messages when they were specifically discussing stealing company property. . . . [t]he company couldn't decrypt the messages. The employees got caught because . . . [an] investigative company found a Microsoft PowerPoint presentation about their new company in the system." Emily Leinfuss, *Policy Over Policing: It's Easy to Develop E-mail and Internet Policies, but Education and Documentation are Crucial to Their Success*, INFOWORLD, Aug. 19, 1996, at 56.

181. *See* Araneo, *supra* note 12, at 343.

dence in litigation and may be discoverable on a firm's server or in back-up tapes.[182] These possibilities provide the firm with the justification that e-mail users' privacy interests are limited by these more important concerns for the firm.[183]

1. Policies Created by Businesses

The solution that most commentators and business people have provided for the resolution of e-mail monitoring is for firms with e-mail systems to self-regulate by establishing and creating internal policies for users of the firm's e-mail system. The rationale for the creation of such policies is several fold. First, the creation of a policy puts users of the system on notice that the firm is going to monitor the e-mail system. Once such notice is given, a user of the system is consenting to the firm's monitoring of the system. Second, the policy provides users with a clear understanding of the firm's expectation of how the e-mail system can be used and what types of messages are appropriately sent on the firm's e-mail system. The policy also tells users that " '[t]he system is in place to facilitate the employees doing their job.' "[184] One commentator has noted that "[a]n E-mail policy will help prevent abuse or misuse of the E-mail system, clarify privacy expectations, reduce tensions about privacy invasion, and help to avert possible legal action."[185] Another has noted that the purpose of internal e-mail monitoring policies is to "provide notice to the employees of exactly what rights are granted to them and those that remain vested in the employer. This in turn, clearly informs the employees as to what type of environment they are in, and how to act accordingly."[186]

2. Model Policies

The literature is replete with examples of the exact wording of such policies and proposed model policies.[187] One such example of an e-mail policy includes the following suggested provisions:

---

182. *See* Olmstead, *supra* note 9, at 523.

183. Additionally, one commentator states that "traditional" tort claims in the context of new workplace technologies, using the new term "techno-torts" to describe such actions, are more complex and difficult for businesses to successfully litigate. *See* Martin C. Loesch, *Recent Developments in Self-Insurance and Risk Management*, 32 TORT & INS. L.J. 583, 585 (1997).

184. Soden, *supra* note 4, at 19.

185. WILLIAM S. HUBBARTT, THE NEW BATTLE OVER WORKPLACE PRIVACY 144 (1998).

186. Araneo, *supra* note 12, at 357.

187. For an extensive list of elements to consider when proposing policies *see id.* at 362–64.

> (a) that the e-mail system should be used for business purposes only; (b) that e-mail messages are automatically stored on the computer's back-up system; and, (c) that all e-mail messages are subject to review by the Company's management from time to time or at any time at management's discretion.[188]

Other "model" e-mail policies are more detailed, such as the Electronic Messaging Association's book, Access to and Use and Disclosure of Electronic Mail on Company Computer Systems: A Tool Kit for Formulating Your Company's Policy.[189] This "Privacy Tool Kit" provides several checklists and questions to help companies in formulating a policy.[190] The book also provides four draft policies, each of which takes a different approach to the limits and scope of access to workplace e-mail.[191] The policies are organized in a continuum from least protective of employee rights to most.[192] The first draft policy is entitled "No Restraint on Access or Disclosure" which in part states that: "All messages are company records. The company reserves the right to access and disclose all messages sent over its electronic mail system for any purpose."[193] The least restrictive policy is the "Policy Establishing Bright Line Rules Preventing Particular Types of Access and Disclosure and Requiring Notice and/or Approval by Employees," which states in part that: "The company provides electronic mail to employees, at company expense, for their use on company business and incidentally for personal purposes."[194]

Some corporations have policies of the "No Restraint of Access or Disclosure" type, some have policies of the more permissive type, and still others have no policy regarding access to firm e-mail messages.[195] Due to the current state of the law, firms are at liberty to choose which policy to adopt and how to enforce such a policy. As far as the ECPA is concerned, as interpreted by courts in *Bohach* and *Andersen*, so long as the firm is an e-mail provider, the user's firm e-mail can be accessed.[196]

---

188. C. Forbes Sargent, *Electronic Media and the Workplace: Confidentiality, Privacy and Other Issues*, BOSTON BAR JOURNAL, May/June 1997, at 6, 20.

189. DAVID R. JOHNSON ET AL., ACCESS TO AND USE AND DISCLOSURE OF ELECTRONIC MAIL ON COMPANY SYSTEMS: A TOOL KIT FOR FORMULATING YOUR COMPANY'S POLICY (1994)

190. *See id.* at 3-29.

191. *See id.* at 31–38.

192. *See id.*

193. *Id.* at 31.

194. *Id.* at 37.

195. *See* Pallasch, *supra* note 1, at 4.

196. *See Bohach*, 932 F. Supp. at 1236; *Andersen*, 991 F, Supp. at 1043; *see also* discussion *supra* Part II.A.

C. *Protecting Workplace E-Mail Privacy*

Should people have protections for their e-mail communications in the workplace? Most employers answer this question as maybe or no.[197] Outside of the employee/employer paradigm, looking at this issue from the standpoint of all people in a workplace environment using e-mail, what type of user privacy interest protection should be given to e-mail? In today's society, where people spend many hours a day at work and the lines of distinction are blurred between when a person is at work and at home,[198] people need to have some type of privacy protections in the workplace to protect against other people in the workplace accessing their private e-mail communications.

The workplace is a community. The modern conception of the invasion of privacy tort is that it not only provides people with a remedy for violations of an interest but also allows people to define boundaries and to define what type of conduct can take place within those boundaries. This applies equally to "employees" and "employers." As Post has stated about the tort of intrusion: "It rests on the premise that the integrity of individual personality is dependent upon the observance of certain kinds of social norms."[199] Some businesses even recognize that personal e-mail communications in the workplace have become a social norm, " 'the workplace is an environment of mutual trust and respect,' said Michael Kaminsky, an administrator in G.M.'s systems department [commenting on General Motor's "hand's off" e-mail policy]."[200] The current approach that should be taken is to view workplace e-mail as something that should be protected and something that needs to be protected for all users.

---

197. "[E]mployers often believe that workers have no privacy rights on the company online system. . . ." LANCE ROSE, NETLAW: YOUR RIGHTS IN THE ONLINE WORLD 179 (1995).

198. The clearest example of this blurring between the home and the office is for people who "telecommute" or work at home during part of a work week. These people do not just take some work home on occasion but do substantive amounts of work from their home, which causes there to be less of a distinction between being "at work" and "at home." "[T]he lines between personal and business time have blurred. Personal business happens in the daytime. Employees take work home and don't charge the company for the use of their personal desks and telephones. If the company asks for the latter, it shouldn't complain about the former." Lewis, *supra* note 170.

199. Post, *supra* note 13, at 962.

200. *See* Pallasch, *supra* note 1, at 4. "[UPS and Baxter Healthcare Corp.] say they never read messages routinely. In fact, UPS says it has only read an employee's messages once, when an employee was suspected of accessing and reading other employees' E-mail. By monitoring messages, UPS proved its case." Linda Wilson, *Addressing E-Mail Rights*, INFORMATIONWEEK, Feb. 15, 1993.

1. Policies Created by Businesses

Firms and commentators point to policies created by the firm as the way to go. These policies would generally inform the employee that the firm owns the e-mail system, the e-mail system is only to be used for work, and there is no expectation of privacy for e-mail messages on the firm's system.[201] The majority view is that these policies will indemnify the firm from any liability resulting from the e-mail user's messages or liability from accessing the user's messages.[202] The rationale being that even if the current interpretation of the ECPA's § 2701 exceptions change, a firm will still be protected from liability toward a user because the firm's e-mail policy has put a user on notice that their messages are monitored and that the user's continued use of the e-mail system is an acceptance of this policy. With these policies in place, the firm will be able to monitor employee e-mail and the e-mail using employees will conform their actions to the realities of e-mail message monitoring.[203]

The anecdotal evidence suggests that users are not limiting their e-mail communications in the workplace. E-mail users, while becoming more informed about the technology of e-mail and its accessibility by others, despite password only access to systems, continue to send messages and information via e-mail that they view as being private. Because of the features of e-mail communication, such as speed, ease of use, lack of geographic and temporal limitations, and prevalence in modern communications, users' perceptions of privacy will not easily be changed, regardless of firm policy.[204] In this way, the telephone provides a similar example, because it continues to be used on a daily basis to make and receive personal phone calls at the office.

E-mail users' expectations about the privacy of their e-mail communications may be difficult to change and should not be changed. In

---

201. "Many companies sanctimoniously proclaim that because [e-mail and Internet access are] corporate resources, employees have no right to use them for personal business and should harbor no expectation of privacy. Well, yes, they are corporate resources. So are desks and interoffice mail. Does this mean employees should expect their supervisors to search through both whenever they feel like it?" Lewis, *supra* note 170.

202. "[E]mployers who wish to obtain the most effective protection against employee E-mail privacy claims should publish an E-mail policy that defines the company's rights to review employee E-mail messages." Baumhart, *supra* note 128, at 947.

203. "Informing employees of potential privacy intrusions, however, will not substantially alleviate the extent of unwanted workplace privacy intrusions because most employees do not bargain over working conditions in their employment positions." Gantt, *supra* note 53, at 407.

204. "Under a policy prohibiting personal E-mail communications, employees will undoubtedly experience the resentment and dehumanization that monitored employees often experience on the job." *Id.* at 406; *see also* Marx, *supra* note 18, at 67.

today's world, where people are expected to do work at home or have established an arrangement to do most of their work from home, which is the direct result of technology such as e-mail, affording all people a workplace privacy interest in e-mail communications only enhances the ability of all people to perform their work. The old view that individual privacy is protected at home, but not afforded the same level of protection in the workplace does not work where the distinction between "work" and "home" is blurred or does not exist at all. This idea of a double standard of privacy does not work because users cannot distinguish among "the obligations owed by members of a community to each other,"[205] with the result that people will be less inclined to use the very technology, e-mail, that has become so important to work. Individual firm policies that do not recognize the e-mail users' privacy interest only perpetuate the double standard of privacy and do nothing to define the workplace community other than to mandate unyielding firm dominion over e-mail systems and users' communications.

The varying policies established by individual firms also provide e-mail users with a confusing set of policies and in some cases tell the users that they have no privacy interest, when the users view themselves as having such. In some cases the policies may be misapplied. *Smyth* is such an example.[206] Pillsbury told Smyth and his fellow e-mail users that their communications, via e-mail, would be confidential and privileged and would not be used as the basis for termination;[207] however, then the company acted contrary to its policies.[208] The company accessed his e-mail communications and used them as the basis for his termination.[209]

Flanagan and *Shoars* provide an even clearer example of the downsides of placing a total reliance on policies created by a firm. There, a supervisor decided to monitor everyone's e-mail communications, and when he was discovered, fired the person who caught him, Shoars. The other employees, one of them, Flanagan, whose e-mail communications had been read, also had no legal recourse against Epson. In these cases, the policies of the companies did not afford any privacy protection to the e-mail users. There is yet to be a case where firm policies have not provided liability protection to a firm, but this could happen.[210]

---

205. Post, *supra* note 13, at 1008.

206. *See* Smyth, 914 F. Supp. at 101.

207. *See id.* at 98.

208. *See id.*

209. *See id.*

210. "It appears that for at least today, employers have the greater rights when it comes to monitoring conduct in the workplace. We live in a litigious society, and it is always possible that the wrong facts will hit a judge or member of congress, changing managerial rights once again. It cannot be too strongly stated that common sense should be used in deciding

In *Restuccia*, the users of the e-mail system were employees.[211] *Restuccia* would not have been a different case if they had been partners of Burk in the firm. He could have accessed their e-mail communications, because they disagreed with him about some business decision and would have discovered the same material. If Burk Technology had instituted an e-mail policy, this would not have changed the outcome of the case, so that Restuccia and LoRoe would not have a basis to state a claim against Burk. While policies may clarify how the firm views personal e-mail messages, these policies do not resolve the problem.[212]

Additionally, firm policies do not solve the problem of communications coming into the firm. At firm X, their policy states that users' e-mail messages are protected and will not be monitored, but at firm Y, their policy states that the firm reviews all e-mail messages on the firm's server. It would then be possible that a user at firm Y who receives a personal message, that has passed through firm Y's server and been saved, from a user at firm X, could be fired for the receipt of a personal message from his friend at X.

If each firm is allowed to create their own policy this means that individual firms can do whatever they want and the user of the system has only the amount of privacy protection afforded to them under the firm's policy. This approach is inconsistent with privacy notions, even those lesser ones that have been established in the workplace.[213] In *Vernars v. Young*, the Third Circuit Court of Appeals stated that private individuals, in their place of work, "have a reasonable expectation that their personal mail will not be opened and read by unauthorized persons."[214]

Advocates for individual firm policies stress that the e-mail system is a new and potentially powerful way for users to commit torts and

---

how to use technology for workplace monitoring. Experience shows that the greatest law in your favor is not going to persuade a jury when your facts are objectionable." Julienne W. Bramesco, *Employee Privacy: Avoiding Liability in the Electronic Age*, 562 PLI/LIT 515, 529 (1997).

211. *See Restuccia*, 5 Mass L. Rptr. No. 31, at 712.

212. "Some commentators might respond that explicit monitoring policies will minimize problems with privacy concerns because the policies synchronize the E-mail privacy expectations among employers and employees. Armed by their awareness of the scope of possible privacy intrusions in the workplace, employees will quantify the value of privacy in the workplace and bargain for employment that best maximizes their income potential and minimizes the workplace intrusions into privacy interests they value." Gantt, *supra* note 53, at 406–07.

213. "The moral right to privacy . . . can play a vital role in the private sector employment context. A moral right to privacy is grounded in ethics, particularly the ethical principle that each person posses dignity and respect and must be treated as a worthwhile end and not as a mere means. Such a moral right can serve as a challenge to employer actions that are perceived as invasive, unreasonable or demeaning, but not legally tortious by privacy precedent." Cavico, *supra* note 22, at 1345–46.

214. Vernars v. Young, 539 F.2d 966, 969 (3d Cir. 1976)

other types of wrongs such as the misappropriation of trade secrets. These policies created by firms do not really address these issues.[215] Employees harassing other employees is not a new issue in the workplace and a body of law has been developed to address this issue, including the passage of federal laws.[216] The misappropriation of trade secrets is also not a new issue to the workplace and a body of law has also been developed to address this issue.[217] Because of this, these workplace policies seem substantively to do nothing more than strengthen the notion that e-mail is a new medium which firms singularly control.[218] The law as it currently exists does nothing to clarify the e-mail user's privacy interest.

2. New Federal Legislation

The best solution to the problem of workplace e-mail privacy is to enact a new federal statute. Most firms will not be receptive to onerous federal regulation of this area. However, federal regulation is not unheard of in the context of workplace activities.[219] The need for federal regulation in the area of workplace e-mail has already been raised in Congress. One of the stated purposes of the ECPA was to address the issue of the monitoring of new communication technologies, though the ECPA goes only so far. The ECPA was passed in 1986, which looking back on it, was the infancy of the use of new communications technologies. There are not many people in 1986 who could have predicted the rapid growth and prevalence of e-mail use, especially in the workplace, in the decade following the passage of the ECPA.

Some commentators have suggested that the ECPA needs to be rewritten to clarify the entire area of workplace communications, which

---

215. One commentator has stated that: "Allowing employers to limit liability for wrongs committed against third parties using e-mail provided by the employer will encourage employers to develop company policies which employ only limited monitoring . . . ." Lehman, *supra* note 55, at 112.

216. *See, e.g.*, 42 U.S.C. §§ 2000e-2-2000e-3 (1994) (the Act forbids workplace discrimination and harassment for certain classes of people).

217. *See, e.g.*, The Economic Espionage Act of 1996, 18 U.S.C.A. §§ 1831–1839 (West Supp. 1998).

218. "[Employer policies] compromise employee privacy interests by validating a new avenue by which employers may monitor employees." Gantt, *supra* note 53, at 405.

219. Examples of federal regulation of private sector employment relationships include: The Employee Polygraph Act of 1988, 29 U.S.C. §§ 2001–2009 (1994) (the Act generally prohibits the use of polygraph examinations for preemployment screening or during the course of employment); The Americans with Disabilities Act (ADA) of 1990, 42 U.S.C. §§ 12101–12213 (1994) (the Act prohibits discrimination against employees on the basis of their disability and requires employees with disabilities to be accommodated in the workplace); The Fair Labor Standards Act (FLSA) of 1938, 29 U.S.C. §§ 201–219 (1994) (the Act imposes minimum wage and overtime standards on most employers).

would include e-mail, telephones, voice mail and other types of modern communications systems.[220] Such a measure would be very ambitious and most likely would not occur. The ECPA was an amendment to federal wiretapping statutes and encompasses more than just workplace communications.[221] The prevalence of e-mail as a communications technology in the workplace suggests that it is an issue which should more properly be addressed through legislative measures under federal labor and employment laws, not in terms of wiretapping. Also, as the courts have framed the issue, accessing electronically stored e-mail is not a wiretap and does not encompass the ideas of tapping a wire or even "intercepting" a conversation.[222]

The more recent legislative approach to workplace e-mail monitoring, taken by the PCWA legislation, was to group e-mail monitoring with other forms of workplace monitoring. By doing this the law must make general conclusions about e-mail monitoring in the context of these other very different forms of monitoring, such as identification badge monitoring or video surveillance monitoring. Many commentators have argued that this is the proper way to frame the monitoring issue because then federal legislation will be crafted which is broad and can account for new forms of workplace technology which raise monitoring issues.[223] In a perfect world, this might be an optimal solution. However, because workplace monitoring is a rather controversial issue, it is not likely that businesses will support legislation that not only curtails their current practices but also attempts to curtail and proscribe future unknown practices.

Additionally, e-mail and the other forms of workplace monitoring technology present very different issues. The permanence of e-mail is not an issue present in most of the other forms of workplace monitoring. Also, an all-encompassing federal statute may not fully address some of the e-mail privacy issues, which could result in more of the ambiguity that currently exists. E-mail monitoring, unlike other forms of monitoring which are just accessible by a boss or upper management, is more easily accessed by all people in a firm. One example of this is the *Shoars* case, where a mid-level employee gained access to many employees' e-mail messages. Further, the PCWA legislation failed to address how the provisions of the PCWA were going to affect or be af-

220. *See* Julie A. Flanagan, Note, *Restricting Electronic Monitoring in the Private Workplace*, 43 DUKE L.J. 1256, 1271–80 (1994); Bindler, *supra* note 176, at 880–81.

221. *See* S. REP. NO. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. at 3555.

222. *See Bohach*, 932 F. Supp. at 1236; *Moriarty*, 962 F. Supp. at 221.

223. *See* Bindler, *supra* note 176, at 880–81.

fected by the ECPA. New federal legislation for e-mail monitoring must either amend the current ECPA or indicate how it affects the ECPA.

The paramount issue which new legislation must address is to clarify § 2701 of the ECPA. Section 2701, as currently written, is vague and ambiguous, and courts have done little to clarify these ambiguities. New federal legislation must clarify who is a provider of e-mail services and then delineate the rights of the provider to access stored communications. This should be done by creating a completely new statute. However, the current structure of the ECPA can be used as a model for this. A new provision could follow the structure of the ECPA by prohibiting the accessing of stored communications and providing a civil cause of action for the violation of this prohibition, but such a new provision would provide a clear definition of what constitutes being a provider of e-mail services. A new provision would also have various exceptions to this broad prohibition. These exceptions, a consent and "business use" exception, need to be clearly worded and definitive about how they could be invoked.

The new legislation should create a specific exception which states that users must give express consent to message monitoring. The issue of implied consent is troublesome in the context of e-mail monitoring because most users use passwords to access e-mail communications. Implied consent can easily be construed to have been given when someone signs onto an e-mail system containing a statement in the password program that signing onto the system constitutes consent to access messages.

The consent exception should also be limited in time and scope, so that the user is consenting to the firm accessing only the communications that the user has expressly consented to.[224] By requiring express consent, the user will also have notice that the employer is accessing the user's messages and the scope of this access.[225] Because stored e-mail can be searched and sorted in various ways, if a firm has a need to access a user's messages due to a suspicion of some impropriety on behalf

224. Some commentators have argued that e-mail systems are so large and contain so many messages that firms have no incentive to monitor everyone's e-mail messages. They might respond to an express consent provision such as this by stating that it is unnecessary because the shear volume of the systems is a natural constraint upon firms to do large scale monitoring of users' e-mail messages. *See, e.g.*, PAUL M. SCHWARTZ ET AL., DATA PRIVACY LAW 372 (Michie 1996).

225. This idea is called transparency which is one of the concepts underlying the European data protection principles. Professors Paul M. Schwartz and Joel R. Reidenberg, in their book Data Privacy Law, have summarized transparency as the idea that monitoring activities must be "structured in a manner that will be open and understandable." The two European components to transparency are: "notice to individuals of the collection of personal information . . . . [and] consent from individuals . . . ." *Id.* at 15.

of the user, the firm can obtain the user's consent and then search the system thereby accessing only those messages that pertain to the impropriety while not intruding upon the user's other messages. If a user is unwilling or unable to give this consent, the firm could still access the communication, but the user would be given notice of this access. This notice would state the reason for the access, the information to be accessed, and when and for how long the access would take place. These provisions illustrate how the new legislation will allow access to a user's e-mail messages, but in a limited and controlled manner and for a specified purpose.

Likewise, a "business use" exception would be drafted to clarify the definition of who is a provider and to delineate the access to be given to a provider. Systems administrators may need to access the e-mail system for the purpose of operating the system. However, other people at the firm do not have a need to have broad access to the system. Moreover, this exception should not allow broad access for the purpose of individual message monitoring for the content of a message. If such a need exists then it would be gained through the user's consent under the consent exception and not under the "business use" exception.

Even with federal legislation that clarifies access in this manner, firms would be required to adopt individual policies. However, these policies would not be able to preempt or conflict with the proposed federal provisions. The federal provisions would establish a baseline for what type of access may take place and then firms could adopt policies more stringent or more protective of users' e-mail.[226] The federal legislation would mandate that at the minimum firms must establish policies mirroring the federal legislation.

The federal legislation would also provide a remedy to a user when there has been access in violation of the firm's policy. For example, in *Smyth*, when Pillsbury adopted the policy that e-mail communications were confidential and privileged and could not be used as the basis for termination, but then violated this policy, Smyth would have some recourse under the proposed federal legislation. This recourse does not

226. In his article about privacy and health care information, Professor Paul M. Schwartz makes a similar argument about the way in which his proposed statutory solution would establish "a general default rule." Supporting his proposition, Professor Schwartz cites to "the contracts jurisprudence of Ian Ayres and Robert Gertner" where they "have argued that '[s]etting a default rule that least favors the better informed parties creates an incentive for the informed party to bring up the relative contingency in negotiations.'" Professor Schwartz links this idea to his statutory proposal for health care data stating: "This default rule seeks to maximize both the efficient use of information that is already collected and the necessary negotiations between concerned parties regarding use of these data." Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 59 (1997).

have to be the granting of a cause of action. That could be one option, but it should include some way for a user to redress an access violation. One option would be to allow for internal administrative review or a requirement of a mediation process. The purpose of employer policies is to establish a framework inside the firm for the process of accessing e-mail messages within the federal legislation's guidelines. The basis of these policies, unlike those that currently exist, will not be for the employer to assert their uncontrolled dominion over the firm's e-mail system or to completely absolve the firm of liability for its accessing of e-mail messages.

The proposed federal legislation will be the base and the individual firm policies will provide the structure. These policies will define the "boundaries of the community" and reinforce how the community of the firm is going to address access to e-mail communications. Even the proponents of firm self-regulation stress that policies need to define the community of the firm in terms of access to e-mail communications. The advantage of having both federal legislation which establishes the basic protections in conjunction with firm policies is that the firm retains the ability to gain access to e-mail messages and retains autonomy over the firm's e-mail system. This allows users of the e-mail system to retain their autonomy over message content, while allowing the firm to provide employees with recognition of a privacy interest in their e-mail communications.[227] At the same time, the users will have affirmative knowledge about the type of monitoring that is permissible and possible. The user would also know that some recourse is available for violations of the firm's policy or for violations of the federal legislation.

If a user were to send harassing messages or e-mail messages containing trade secret information on the firm's system, the firm through the user's consent could access those communications and then resolve those issues based upon laws concerning the specific activity. The policies of the firm would apply to all users of the e-mail system and the federal legislation would apply to all workplace e-mail. This would include intranet systems as well as Internet systems. Legislation of this sort should be allowed under Congress' interstate commerce clause power, because e-mail systems, including internal ones, now clearly have an impact on interstate commerce even under the current Supreme

227. "[P]rivacy is best protected when monitoring is minimally intrusive, is directly relevant to job performance, and is visible. . . . Highly intrusive forms of checking that are not directly related to work output should be restricted to situations where there are some grounds for suspicion." Marx, *supra* note 18, at 72.

Court's more limiting interpretation of this power in light of *United States v. Lopez*.[228]

CONCLUSION

The technology of e-mail poses the new workplace privacy issue of who should be able to access e-mail users' workplace e-mail communications. All e-mail users have a privacy interest in these communications because being able to communicate privately in this new medium has become a recognized social norm. Users, despite admonitions to do otherwise, continue to transmit private messages and information via e-mail. Moreover a privacy interest must also be afforded to e-mail communications to provide users with a sense of community and to establish boundaries within this boundless community.

The ECPA, as originally enacted, was supposed to provide protection against the general monitoring and interception of e-mail messages except through limited exceptions. However, judicial interpretation has left the Act with no protections for workplace e-mail users. Additional federal legislation that has thus far been proposed seems destined to further leave workplace e-mail users without any meaningful protection of their privacy interest in workplace e-mail. In order for there to be recognition of the workplace privacy interest in e-mail communications, new federal legislation must be passed, which while mirroring the ECPA, will close the large loopholes of the ECPA's consent and "business use" exceptions.

Until federal legislation along these lines becomes law, workplace e-mail users have the remedy of the common law invasion of torts as their only available remedy, in some cases, against egregious intrusions into their private communications. With the law in this state, it remains to be seen whether e-mail use will continue to grow and become the preferred mode of communication, as it has done since its recent introduction, or whether it will wither as e-mail users revert to modes of communication with more clearly recognized privacy interests.

---

228. United States v. Lopez, 514 U.S. 549 (1995) (finding that Congress's commerce clause power was too attenuated in enacting the Gun-Free School Zones Act of 1990). Internet and intranet e-mail systems have become integral to the way in which most firms transact their daily business, so much so that just because a communication may not cross an interstate boundary the communications system still has an impact upon the way in which that firm transacts its business. For a discussion about the possible application of the Commerce Clause to the regulation of computer bulletin boards in the context of the regulation of cyberporn, see Glenn Harlan Reynolds, *Virtual Reality and "Virtual Welters": A Note on the Commerce Clause Implications of Regulating Cyberporn*, 82 VA. L. REV. 535, 537 (1996).