Volume 8, Number 2 Spring 1995

AN AFFRONT TO HUMAN DIGNITY: ELECTRONIC MAIL MONITORING IN THE PRIVATE SECTOR WORKPLACE

Larry O. Natt Gantt, II[*]

"Laws and institutions must go hand in hand with the progress of the human mind . . . . [A]s new discoveries are made . . . institutions must advance also, and keep pace with the times."[1]

INTRODUCTION

Although employers have historically monitored their employees,[2] the current widespread development of sophisticated technology is greatly expanding the advanced and highly effective methods by which employers monitor the workplace.[3] As these technological advances are frequently designed for or quickly adapted to the demands of the work environment,[4] modern offices are becoming "electronic sweatshops."[5] For instance, the

---

* J.D., Harvard Law School, 1994; A.B., Duke University, 1991. The author is a clerk to Judge Donald S. Russell, United States Court of Appeals for the Fourth Circuit.

1. 2 THE JEFFERSONIAN CYCLOPEDIA: A COMPREHENSIVE COLLECTION OF THE VIEWS OF THOMAS JEFFERSON 726 (John P. Foley ed., 1967).

2. David F. Linowes & Ray C. Spencer, *Privacy: The Workplace Issue of the '90s*, 23 J. MARSHALL L. REV. 591, 597 (1990) (citing DAVID F. LINOWES, PRIVACY IN AMERICA: IS YOUR PRIVATE LIFE IN THE PUBLIC EYE? 31 (1989)) (noting an example from the early twentieth century in which the Ford Motor Company utilized a sociological department to monitor the workers' behavior outside the workplace); *see also* Holly Metz, *They've Got Their Eyes on You*, STUDENT LAW., Feb. 1994, at 22, 24 (noting that personal observation and recording of worker performance began during industrialization).

3. *See, e.g.*, Robert B. Fitzpatrick, *Privacy Issues in the Electronic Monitoring and Surveillance of Employees*, C742 A.L.I.-A.B.A. COURSE STUDY 1165, 1167 (1992), *available in* WESTLAW, ALI-ABA database [hereinafter Fitzpatrick (1992)]; Jennifer J. Griffin, *The Monitoring of Electronic Mail in the Private Sector Workplace: An Electronic Assault on Employee Privacy Rights*, 4 SOFTWARE L.J. 493, 494 (1991); Michael F. Rosenblum, *The Expanding Scope of Workplace Security and Employee Privacy Issues*, 3 DEPAUL BUS. L.J. 77, 96 (1990); Hannibal F. Heredia, Comment, *Is There Privacy in the Workplace?: Guaranteeing a Broader Privacy Right for Workers Under California Law*, 22 SW. U. L. REV. 307, 330 (1992); Note, *Addressing the New Hazards of the High Technology Workplace*, 104 HARV. L. REV. 1898, 1898 (1991).

4. Michael W. Droke, *Private, Legislative and Judicial Options for Clarification of Employee Rights to the Contents of Their Electronic Mail Systems*, 32 SANTA CLARA L. REV. 167, 168 (1992).

5. Catherine Collins, *Bill Would Require Notices When Bosses Snoop on Employees*, L.A. TIMES, Nov. 3, 1991, at D2 ("'[u]nrestrained surveillance of workers has turned many modern offices into electronic sweatshops'") (statement of Sen. Paul Simon (D-Ill.)); *see* Kenneth A. Jenero & Lynne D. Mapes-Riordan, *Electronic Monitoring of Employees and*

National Institute for Occupational Safety and Health has estimated that sixty-six percent of all computer operators, or approximately twenty-six million workers, are subject to electronic monitoring by their employers.[6] A more recent 1993 survey of employers found that "[a]bout 22 percent . . . have engaged in searches of employee computer files, voice mail, electronic mail, or other networking communications" and that "[i]n companies with 1000 or more employees, the figure rises to 30 percent."[7]

These new monitoring technologies have intensified employee privacy concerns because the instruments abolish the desirable balance of power between employers and employees.[8] The instruments allow employers to invade the personal lives of employees with little or no chance of detection.[9] Furthermore, electronic monitoring allows employers to manipulate, access, and collect information about employees in greater amounts than previously possible.[10]

Employee privacy concerns have been compounded by the ability of new technology to outpace existing legal sources of privacy protection, as courts seem either unwilling or unable to protect employees from purely electronic invasions of privacy.[11] Some delay in the law is

---

the Elusive "Right to Privacy," 18 EMPLOYEE REL. L.J. 71, 71-72 (1992) (noting that monitoring will steadily increase as it becomes cheaper to perform).

6. Fitzpatrick (1992), *supra* note 3, at 1169 (citing OFFICE OF TECHNOLOGY ASSESSMENT, ELECTRONIC SUPERVISOR: NEW TECHNOLOGY, NEW TENSIONS 124-25 (1987)). Other statistics estimate that every year only six to ten million employees nationwide are monitored by their employers by computer systems that track performance and monitor information. Julie Gannon Shoop, *Electronic Monitoring: Is Big Brother at the Office?*, TRIAL, Jan. 1992, at 13, 13.

7. Charles Piller, *Bosses with X-Ray Eyes*, MACWORLD, July 1993, at 118, 120 (special report on electronic privacy). From a survey of companies employing a total of one million people, the magazine estimated that 20 million Americans work at places utilizing computer monitoring. The survey also found that only 18 percent of responding companies had a written policy concerning electronic employee monitoring. *Id.*

8. *See* Metz, *supra* note 2, at 28 ("'With new technological advances, the advantages that employers have are becoming almost insurmountable.'") (statement of Robert Ellis Smith, publisher of the *Privacy Journal*); Piller, *supra* note 7, at 121; *see also* Robert B. Fitzpatrick, *Privacy Issues in Surveillance, Search, and Monitoring of Employees*, C669 A.L.I.-A.B.A. COURSE STUDY 23, 36 (1991), *available in* WESTLAW, ALI-ABA database [hereinafter Fitzpatrick (1991)] (noting that the stress experienced by monitored employees is due, in part, to direct and contemporaneous monitoring by supposedly precise methods).

9. *See* Frank J. Cavico, *Invasion of Privacy in the Private Employment Sector: Tortious and Ethical Aspects*, 30 HOUS. L. REV. 1263, 1265 (1993); Jenero & Mapes-Riordan, *supra* note 5, at 71.

10. Griffin, *supra* note 3, at 507.

11. *See* Linowes & Spencer, *supra* note 2, at 598 (citing DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 4 (1989)); Steven B. Winters, *Do Not Fold, Spindle or Mutilate: An Examination of Workplace Privacy in Electronic Mail*, 1 S. CAL. INTERDISCIPLINARY L.J. 85, 86-87 (1992) [hereinafter Winters (1992)].

understandable given that the law is reactive and legislatures and courts cannot anticipate all the problems associated with new workplace technologies.[12] As technology develops in sophistication, however, commentators debate whether modern technology has given the employer so much control over the workplace that the balance of power between employees and employers must be readjusted by law to ensure adequate employee privacy.[13] The new technologies have thus generated a fundamental uncertainty concerning the privacy rights of employees,[14] as the freedom from monitoring by one's employer is increasingly perceived as being outside the scope of reasonable privacy expectations.[15]

The result of this legal lethargy has been that employees must rely on employer self-regulation to protect their privacy interests.[16] This solution is unacceptable because employers often believe they have significant incentives to marginalize the protection of employee privacy.[17] Consequently, American businesses have largely failed to revise their in-house privacy policies despite their increasing use of electronic monitoring.[18] This enlarging gap between employee privacy interests and employer monitoring policies is undoubtedly reflected in the marked increase in employee suits alleging invasion of privacy by employers.[19] The legal delay must thus be minimized in order to maximize accuracy, justice, and efficiency when litigating employee privacy issues.[20]

---

12. Winters (1992), *supra* note 11, at 89. Winters also explains why the law lags behind computer technology by discussing Professor Laurence Tribe's arguments that courts continue to make outdated law because they adjudicate issues based on an old paradigm's notion of privacy. Winters thus reasons that a paradigmatic shift should occur to modernize legal notions of privacy. *See id.* at 89-94.

13. *See* Linowes & Spencer, *supra* note 2, at 598 (citing Fred Weingarten, *Communications Technology: New Challenges to Privacy*, 21 J. MARSHALL L. REV. 735, 746 (1988)); Winters (1992), *supra* note 11, at 96; Griffin, *supra* note 3, at 494; Linowes & Spencer, *supra* note 2, at 591; Kurt H. Decker, *Employment Privacy Law for the 1990's*, 15 PEPP. L. REV. 551, 562-64 (1988).

14. Cavico, *supra* note 9, at 1266.

15. Linowes & Spencer, *supra* note 2, at 592.

16. *Id.* at 598 (citing DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 4 (1989)).

17. *See* Martha W. Barnett & Scott D. Makar, *"In the Ordinary Course of Business": The Legal Limits of Workplace Wiretapping*, 10 HASTINGS COMM. & ENT. L.J. 715, 717 (1988); *see also infra* notes 38-40 and accompanying text (giving examples of employer incentives).

18. *See* Linowes & Spencer, *supra* note 2, at 620.

19. Barnett & Makar, *supra* note 17, at 717 (citing BUREAU OF NATIONAL AFFAIRS, WORKPLACE PRIVACY: EMPLOYEE TESTING, SURVEILLANCE, AND WRONGFUL DISCHARGE AND OTHER AREAS OF VULNERABILITY 107-46 (1987) (special report compiling cases involving workplace privacy issues)).

20. Winters (1992), *supra* note 11, at 89.

This battle between employee privacy interests and employer surveillance needs has recently been played out in the context of the increasingly popular medium of electronic mail ("E-mail").[21] Recent estimates speculate that more than twenty million Americans regularly use E-mail at work,[22] with E-mail being used in some capacity by all Fortune 1000 companies[23] and by seventy-five percent of all large companies in America.[24] Commentators predict that by the year 2000, an estimated forty million users will send sixty billion E-mail messages a year.[25] Especially in companies in which much work is performed on computers, E-mail has become a strategic communications backbone.[26] E-mail has achieved this status because the employer gains numerous benefits through the use of E-mail technology, such as increasing employee productivity[27] and saving money over comparable mail or facsimile costs.[28]

As E-mail grows in popularity, opponents of employer E-mail monitoring assert that the increased monitoring will undermine E-mail

---

21. *See* Note, *supra* note 3, at 1909; *see also* Metz, *supra* note 2, at 23. For a discussion of how E-mail systems operate, see, e.g., Droke, *supra* note 4, at 169-70. One aspect of E-mail worth highlighting is the fact that E-mail systems differ as to whether they copy messages as the messages pass through the system or whether they eliminate the messages automatically. If the messages are copied, E-mail systems, unlike telephone systems, create a document that survives the receiver's deletion of the message. *Id.* at 170. For purposes of this article, I am analyzing the type of E-mail system that allows users to send their messages only to selected recipients. I am not addressing electronic bulletin boards that automatically broadcast messages to all users.

22. *Electronic Mail Raises Issues About Privacy, Experts Say*, DAILY LAB. REP., Nov. 17, 1992, at A7. This figure represents an increase from 430,000 in 1980. Bruce Caldwell, *Big Brother Is Watching: Can Companies Secretly Monitor Their Employees' Electronic Mail?*, INFO. WK., June 18, 1990, at 34.

23. Winters (1992), *supra* note 11, at 87 (citing Walter Ulrich, *Rights of Privacy on Electronic Mail*, L.A. TIMES, Mar. 6, 1991, at D3).

24. Amy Kuebelbeck, *Getting the Message: E-mail Is Fast and Efficient*, L.A. TIMES, Sept. 4, 1991, at E1.

25. Laurie Thomas Lee, *Watch Your E-Mail! Employee E-Mail Monitoring and Privacy in the Age of the "Electronic Sweatshop,"* 28 J. MARSHALL L. REV. 139, 139-40 (1994).

26. Droke, *supra* note 4, at 178 (citing Joanie M. Wexler, *Users Find Frustration in Bulky E-mail Links*, COMPUTERWORLD, Apr. 30, 1990, at 55); *see also* Note, *supra* note 3, at 1909.

27. *See* Michele C. Kane, *Electronic Mail and Privacy*, PRAC. L. INST. PATS. COPYRIGHTS TRADEMARKS LITERARY PROP. COURSE HANDBOOK SERIES, Oct.-Nov. 1993, at 419, 438 (noting that E-mail avoids the problems of telephone tag and time zone dissonance); Griffin, *supra* note 3, at 498-99 (stating that E-mail increases productivity by encouraging more succinct communications among employees); Note, *supra* note 3, at 1909 (noting that E-mail fosters efficient decisionmaking).

28. Kane, *supra* note 27, at 438; *see also* Griffin, *supra* note 3, at 499 (stating that E-mail systems are relatively inexpensive). In addition to the benefits discussed in the text, E-mail also improves client service if clients can tie in directly to the employer's E-mail. *See* Jon Klemens, *The Argument for E-Mail*, LAW PRAC. MGMT., Nov./Dec. 1990, at 38.

benefits in the absence of further privacy protection.[29] Indeed, E-mail's unique position between traditional business communications, such as internal memoranda, and traditional private communications, such as personal letters[30] and telephone calls,[31] creates a tension that ultimately compromises employee privacy.[32] Conflict arises between employers and employees largely because of their divergent expectations regarding the proper use of E-mail.[33] Employees consider their E-mail messages to be their private property, and they use E-mail to send private messages to co-workers.[34] Many employees remain unaware that even though their system may require a username and password to gain access to E-mail files, the central computer routing the messages stores the transmissions in unencrypted plain text files[35] available to the service provider, whether

---

29. Griffin, *supra* note 3, at 500-01. E-mail monitoring may occur at several stages in the course of composing, sending, and receiving the message. First, the contents may be accessed from the sender's computer terminal, either by looking directly at the screen or by accessing the sender's E-mail file. Second, the contents may be intercepted during transmission, either by an unauthorized wiretap or by the central computer which routes the messages. Third, the contents may be accessed at the recipient's terminal, either by direct display on the screen or by accessing the recipient's E-mail file. Additionally, at most if not all of the stages, the transmissions may be printed into hardcopy. *Id.*

30. Mail carried through the U.S. Postal Service is afforded a high degree of protection against unauthorized opening. *See* United States v. Van Leeuwenm, 397 U.S. 249, 251 (1970).

31. Numerous cases have adjudicated privacy protections regarding telephone communications. *See, e.g.*, Nader v. General Motors Corp., 255 N.E.2d 765, 770 (N.Y. 1970) (holding that the interception of private phone conversation violated the invasion of privacy tort).

32. Note, *supra* note 3, at 1909.

33. *Id.*

34. *Id.* at 1909-10; *see also* OFFICE OF TECHNOLOGY ASSESSMENT, ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 50 (1985) [hereinafter OTA, ELECTRONIC SURVEILLANCE]; Yvonne Lee, *Controversy over Privacy of Electronic Mail Sparks Lawsuit Against Nissan Motors*, INFOWORLD, Jan. 14, 1991, at 5, 5.

35. Griffin, *supra* note 3, at 499 (citing Simson L. Garfinkel, *Use E-mail for Efficiency*, 35 PRAC. LAW. 41, 47 (1989)); Heredia, *supra* note 3, at 331 (citing OTA, ELECTRONIC SURVEILLANCE, *supra* note 34, at 48). Protection against the message's content being exposed by the central computer is available through encryption software. This technology allows senders to encrypt messages prior to transmission and recipients to decrypt messages upon receipt. Although the cost of encryption software initially was excessive, Griffin, *supra* note 3, at 500, encryption programs are now widely available from various sources including the Internet. *See* Peter H. Lewis, *Between a Hacker and a Hard Place: Data-Security Export Law Puts Businesses in a Bind*, N.Y. TIMES, Apr. 10, 1995, at C1, C6. Utilizing encryption software in the workplace does not represent a promising option to protect employee privacy because employers would presumably retain the decoder key needed to access employee electronic communications. Additionally, the legality of certain encryption software is uncertain given that the federal government is currently regulating the proliferation of advanced encryption software because it is concerned about protecting its ability to decode private communications for law enforcement purposes. *See id.*

that be a third-party common carrier or the employer itself.[36] In contrast, employers claim that E-mail is a resource to be used solely for business activities and therefore the communications, as part of the E-mail system, are the property of the business.[37] Employers further assert business justifications for monitoring their employees' E-mail, such as reducing personal communications;[38] improving the work-product; protecting against theft, fraud, and computer crime;[39] and otherwise remaining viable in a competitive market.[40]

This Article examines the existing legal sources protecting the privacy interests of employees whose employers monitor employee E-mail communications. Although the examination addresses employers who monitor employee E-mail communications transmitted over common-carrier networks, the analysis concentrates on employers who monitor communications on networks they own and operate. This Article determines that the existing legal protections do not adequately safeguard employee privacy interests in E-mail transmissions. This Article reasons that these sources all remain inadequate largely because they fundamentally condition privacy protection on the employee's expectation of privacy and a balancing of that protection that defers to the employer's legitimate business interests in monitoring its employees.

This Article concludes that further federal legislation must be enacted in order to protect employees from abusive employer E-mail monitoring practices. In order for such legislation effectively to address the privacy interests at stake, this Article reasons that future legislation must abandon the relative standards that condition employee privacy rights on the actions and interests of their employers. This Article concludes that future legislative solutions must instead return to the traditional notions of privacy as an independent legal right designed to protect human dignity and respect for individuals.

---

36. Griffin, *supra* note 3, at 499 (citing Garfinkel, *supra* note 35, at 46-47).

37. *See* Note, *supra* note 3, at 1910; Heredia, *supra* note 3, at 332. Employers further contend their interest should be favored because employees normally work on employer premises, employers often own the workplace communications equipment, and company business is conducted on the equipment. Winters (1992), *supra* note 11, at 95-96. These arguments are relevant to employers who purchase and maintain their own E-mail systems.

38. Note, *supra* note 3, at 1910 (citing, inter alia, Alice LaPlante, *Is Big Brother Watching?*, INFOWORLD, Jan. 14, 1991, at 58).

39. *See* Winters (1992), *supra* note 11, at 95-96.

40. Barnett & Makar, *supra* note 17, at 717.

I. ELECTRONIC COMMUNICATIONS PRIVACY ACT

Existing federal statutes regulating computer crimes[41] and informational privacy[42] do not explicitly govern the ability of private employers to monitor employee E-mail communications.[43] The only federal statute that specifically addresses the interception and accession of E-mail communications is the Electronic Communications Privacy Act of 1986 ("ECPA"),[44] which amended Title III of the Omnibus Crime Control and Safe Streets Act ("Title III").[45] In order to close the Title III loopholes, Title I of the ECPA expands Title III's prohibition of the unauthorized interception of wire and oral communications to include electronic communications.[46] The legislative history evidences a clear congressional intent that E-mail be considered within the definition of electronic communications.[47] Title I of the ECPA also prohibits the intentional disclosure, attempt to disclose, or other use of information obtained from an unauthorized interception if the person using the information knew or had reason to know that the information was obtained illegally.[48] The

---

41. *See* The Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1001 (1988).

42. *See Privacy Statutes on File*, 21 NAT'L L.J. 2520 (1989). Congress has enacted numerous statutes addressing privacy concerns arising from the development of various information technologies. *Id.*

43. Griffin, *supra* note 3, at 512-13.

44. Pub. L. No. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C.).

45. 18 U.S.C. §§ 2510-2520 (1988). Congress evidenced no intent that the ECPA would preempt other sources of liability for employers who peruse employee E-mail messages. Julia T. Baumhart, *The Employer's Right to Read Employee E-mail: Protecting Property or Personal Prying*, 8 LAB. LAW. 923, 932, 937 (1992). The impetus for enacting the ECPA derived from a 1985 report from the Office of Technology Assessment, which emphatically expressed the threat to privacy posed by unregulated invasions into electronic communications. Kane, *supra* note 27, at 427; Baumhart, *supra*, at 924.

In addition to the ECPA, only one federal statute, the Communications Act of 1934, has been identified to date as having potential parallel applicability to electronic communications in the employment context. It is doubtful today, however, that a court would sustain a cause of action under the Communications Act when the underlying claim is based on disclosure permitted by the ECPA. Baumhart, *supra*, at 938-39.

46. 18 U.S.C. § 2511 (1988). The ECPA defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate commerce." 18 U.S.C. § 2510(12) (1988).

47. "Communications consisting solely of data, for example, and all communications transmitted only by radio are electronic communications. This term also includes electronic mail, digitized transmissions, and video teleconferences." S. REP. NO. 541, 99th Cong., 2d Sess. 14 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568 [hereinafter ECPA Legis. Hist.].

48. 18 U.S.C. § 2511(1)(c) (1988).

legislative history reveals that the requisite mens rea is that the damaging interception must be the "conscious objective" of the intercepter.[49]

Title I of the ECPA also broadens the Title III definition of the term *interception* to cover non-aural acquisition by defining the term as the "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[50] The statutory definition of *contents* does not include data identifying details of telecommunications, such as E-mail transactional information,[51] and the ECPA does not require that the interception be contemporaneous with the transmission.[52] This protection from interception covers intentional actions to intercept communications by unauthorized individuals and individuals acting on behalf of the government.[53] From this emphasis on "third party" interception, the ECPA does not explicitly offer protection from employers who access or intercept the electronic communications of their employees.[54] The Act instead provides protection in situations where an employee or outside individual exceeds his or her authority when accessing, intercepting, or disclosing information on a private corporate system.[55] This focus implies that, in enacting the ECPA, Congress was primarily concerned about protecting corporations against their competitors that might desire to steal valuable electronic information. Nothing in the ECPA legislative history, however, evidences any clear congressional intent that the Act should not be read to cover private employer monitoring of employee E-mail communications.[56]

---

49. ECPA Legis. Hist., *supra* note 47, 1986 U.S.C.C.A.N. at 3577.

50. 18 U.S.C. § 2510(4) (1988).

51. "'[C]ontents,' when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (1988).

52. While the ECPA is silent on any requirement that interception and transmission be simultaneous, the ECPA legislative history generally references an Office of Technology Assessment report which lists five different times when an E-mail message can be intercepted. ECPA Legis. Hist., *supra* note 47, 1986 U.S.C.C.A.N. at 3557-58 (discussing OTA, ELECTRONIC SURVEILLANCE, *supra* note 34, at 48).

53. 18 U.S.C. § 2511(1)(a), (2)(a)(ii)(A) (1988). A government agent generally must have a court order that directs the service provider to assist and intercept the communication and is signed by a judge who has authority to direct such an interception. *Id.*

54. Winters (1992), *supra* note 11, at 119.

55. *See* Ruel Torres Hernandez, *ECPA and Online Computer Privacy*, 41 FED. COMM. L.J. 17, 38 (1988); *see also* ECPA Legis. Hist., *supra* note 47, 1986 U.S.C.C.A.N. at 3590.

56. Winters (1992), *supra* note 11, at 119.

In addition to Title I's protection against interception, Title II of the ECPA protects against the accession of electronic communications, such as E-mail messages, that are stored in a computer system for later retrieval.[57] Title II prohibits breaking into an electronic storage system by anyone who is intentionally accessing the system without authorization, or is intentionally exceeding authorized access into the system.[58] Similarly, Title II prevents law enforcement officials from invading an electronic storage system without a court order, absent exigent circumstances.[59] Any violation of the Act gives rise to both criminal and civil liability, and an employee may therefore recover damages by successfully showing that an employer violated the ECPA in intercepting, disclosing, or accessing an E-mail communication.[60] In sum, a prima facie violation of the ECPA entails the defendant's intentional or willful interception, accession, disclosure, or use of the plaintiff's wire, oral, or electronic communication, where the interception occurred on the premises of a business the operation of which affected interstate commerce.[61]

---

57. "Electronic storage" is defined as: "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17) (1988); *see also* Baumhart, *supra* note 45, at 925.

58. 18 U.S.C. § 2701(a) (1988). For instance, an unauthorized invasion would occur if an employer authorized an employee to access information located in his or her E-mail mailbox and that individual accessed information belonging to other subscribers. ECPA Legis. Hist., *supra* note 47, 1986 U.S.C.C.A.N. at 3590.

59. 18 U.S.C. § 2703 (1988). Delayed notice is acceptable, or notice is not even required, where exigent circumstances exist. The ECPA lists several exigent circumstances: 1) endangering the life or physical safety of an individual; 2) flight from prosecution; 3) destroying or tampering with evidence; and 4) intimidation of a potential witness. 18 U.S.C. § 2705 (1988). Furthermore, the ECPA makes a distinction between electronic communications stored for 180 days or less, for which a government agency needs a federal or state warrant to access, and those stored for more than 180 days, which the government can access more easily without a warrant. 18 U.S.C. § 2703(a)-(b) (1988).

60. A civil plaintiff who proves a violation of the interception provisions may recover the greater of either: (1) actual damages suffered and any profits made by the violator; or (2) statutory damages the greater of $100 a day for each day of violation or $10,000. 18 U.S.C. § 2520(c)(2) (1988). A successful plaintiff may also recover reasonable attorneys' fees, litigation costs, and other equitable relief. 18 U.S.C. § 2520(a)(3) (1988). The criminal penalty for interception violations includes up to five years imprisonment and fines up to $500. 18 U.S.C. § 2511(4)(a)-(b) (1988). A civil plaintiff who proves a violation of the stored communications provisions may recover equitable relief, damages including lost profits with a damage minimum of $1000, and reasonable attorneys' fees and litigation costs. 18 U.S.C. § 2707(a)-(c) (1988). The criminal penalty includes up to one year imprisonment and fines up to $250,000 on the first offense if the offense is committed for commercial advantage or involves malicious destruction or damage or private commercial gain. 18 U.S.C. § 2701(b) (1988).

61. Barnett & Makar, *supra* note 17, at 722 (citing United States v. Duncan, 598 F.2d 839, 847 (4th Cir. 1979), *cert. denied*, 444 U.S. 871 (1980)). In order to satisfy

Important to the discussion of E-mail privacy is Title III's distinction between protected oral communications and protected wire and electronic communications, the latter including E-mail. Title III's definition of "oral communication" is drawn from the principle enunciated in *Katz v. United States*,[62] which protects such communications only when the speaker has a reasonable expectation of privacy.[63] The ECPA, however, protects "wire communications" and "electronic communications" against interception without reference to the privacy expectations of the parties to the communication.[64] Although the parties' subjective privacy expectations are therefore seemingly irrelevant in finding ECPA liability, they remain germane in determining whether an interception is in the "ordinary course of business" under the context approach to the ECPA's business-extension exception, discussed below.[65]

The ECPA includes three primary exceptions to its prohibition against the interception or accession of electronic communications: (1) an exception allowing interception if one of the parties consents;[66] (2) an exception allowing providers of wire or electronic communication services to monitor their lines to ensure adequate service;[67] and (3) an exception

---

constitutional standards, the ECPA includes a qualifier that the Act only applies to communications that affect interstate or foreign commerce. 18 U.S.C. § 2510(12) (1988). Given the expansive judicial interpretation of the meaning of interstate commerce, this limitation presumably will not thwart many, if any, employee privacy claims based on E-mail communications on intracompany networks. *See generally* Heart of Atlanta Motel, Inc. v. United States, 379 U.S. 241 (1964) (applying a broad interpretation of Congress' power to regulate interstate commerce in holding that the public accommodations provisions of the Civil Rights Act of 1964 are valid under the commerce clause). One commentator, however, questions whether the ECPA covers E-mail messages communicated through intracompany networks that do not cross state lines or connect to an interstate network. Lee, *supra* note 25, at 152-53.

62. 389 U.S. 347, 353 (1967).

63. An "oral communication" is defined as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication." 18 U.S.C. § 2510(2) (1988). Title III also allows the interception of oral communications by one of the parties to the communication or where one of the parties has previously consented. 18 U.S.C. § 2511(2)(d) (1988).

64. 18 U.S.C. § 2510(1) (1988); *see also* Briggs v. American Air Filter Co., 630 F.2d 414, 417 (5th Cir. 1980) (stating that Title III prohibits unauthorized interception of wire communications regardless of the speaker's privacy expectation).

65. *See* Barnett & Makar, *supra* note 17, at 741; *see also Briggs*, 630 F.2d at 417-18 (reasoning that privacy expectations may be relevant in determining whether certain interceptions are in the ordinary course of business); United States v. Harpel, 493 F.2d 346, 350 (10th Cir. 1974) (determining that consent is to be considered independently of whether an interception occurred).

66. 18 U.S.C. § 2511(2)(c) (1988) (applies to both oral and wire communications).

67. 18 U.S.C. § 2511(2)(a)(I) (1988).

allowing interception if done by a device provided by the communications provider or subscriber and done in the intercepter's "ordinary course of . . . business."[68] Currently, several reported cases have applied the ECPA in the case of new cellular technologies[69] and display pagers,[70] but only one federal case has explicitly applied the Act to E-mail interception or accession.[71] That case involved the government's ability to seize electronic communications, and the relevance of the opinion to a private employer's monitoring of employee E-mail is limited to its holding that Title I "interception" provisions do not apply to stored electronic communications. An employer unlawfully monitoring E-mail messages would thus be liable under Title I or Title II of the ECPA, but not both, depending on whether the monitored communications were in "electronic storage."[72] This narrow holding, however, does not provide insight into judicial application of the three ECPA exceptions; each of the exceptions is discussed below in its application in analogous contexts in order to ascertain the Act's applicability to employer E-mail monitoring.

---

68. 18 U.S.C. § 2510(5)(a) (1988).

69. *See, e.g.*, United States v. Saurez, 906 F.2d 977 (4th Cir. 1990), *cert. denied*, 498 U.S. 1070 (1991); Shubert v. Metrophone, Inc., 898 F.2d 401 (3d Cir. 1990); Tyler v. Berodt, 877 F.2d 705 (8th Cir. 1989), *cert. denied*, 493 U.S. 1022 (1990); United States v. Ojeda Rios, 875 F.2d 17 (2d Cir. 1989); Edwards v. State Farm Ins. Co., 833 F.2d 535 (5th Cir. 1987).

70. *See, e.g.*, Jackson v. State, 636 So.2d 1372 (Fla. Dist. Ct. App. 1994), *aff'd*, 1995 WL 48439 (Fla. Feb. 9, 1995); Mauldin v. State, 874 S.W.2d 692 (Tex. Ct. App. 1993).

71. Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 461-64 (5th Cir. 1994). Additionally, in Flanagan v. Epson Am., Inc., No. BC007036, slip op. at 5-6 n.1 (Cal. Super. Ct. Jan. 4, 1991), a court addressed whether E-mail interception would be unlawful under the California wiretapping statute. In dictum, the court analyzed in a footnote the applicability of the ECPA provider exception to the case and implied that the exception would exempt the employer from liability. *Id.*; *see infra* notes 358-75 and accompanying text.

72. *Steve Jackson Games*, 36 F.3d at 461-64. In the case, operators and users of a computer bulletin board system alleged, inter alia, that the Secret Service and the U.S. government had violated Title I and Title II of the ECPA by seizing the computer used to operate the bulletin board system, which contained private E-mail messages that had not been read by their intended recipients. The district court held that the Secret Service and the government had violated Title II of the ECPA but had not violated Title I because their seizure did not constitute an "interception" under the terms of the Act. *See* Steve Jackson Games, Inc. v. United States Secret Serv., 816 F. Supp. 432, 441-43 (W.D. Tex. 1993), *aff'd in part*, 36 F.3d 457 (5th Cir. 1994) (addressing only district court's Title I holding).

A. Consent Exception

The first relevant ECPA exception arises when one party to the communication has given prior consent to the interception or accession.[73] The consent exception does not apply if the communication is intercepted "for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State."[74] Furthermore, although the courts have not yet interpreted the consent exception under the stored communications provisions, courts have held that consent under the interception exception may be implied or actual, but that constructive consent is inadequate.[75]

The preeminent case defining the limits of the consent exception is *Watkins v. L.M. Berry & Co.*,[76] which reasoned that employee consent will be carefully limited to the confines of an employer monitoring policy. In *Watkins*, the employer informed its employees that it would monitor their business telephone calls but would monitor their personal calls only to the extent necessary to determine whether a particular call was business or personal. The Eleventh Circuit held that this disclosure constituted employee consent only to the monitoring of business calls and not to the monitoring of the full content of personal calls.[77] The court reasoned that Title III's protections would be thwarted if "consent could routinely be implied from the circumstances." Rather, the court determined that "knowledge of the *capability* of monitoring alone cannot be considered implied consent"[78] and that courts will imply consent when the employee knew or should have known of a policy of constantly monitoring calls, or when the employee conducts a personal conversation over a line that is explicitly reserved for business purposes only.[79]

---

73. 18 U.S.C. § 2511(2)(d) (1988) (interception); 18 U.S.C. § 2702(b)(3) (1988) (access to stored communications). The consent may be given in advance by the originator, the addressee, or the intended recipient.

74. 18 U.S.C. § 2511(2)(d) (1988).

75. Griggs-Ryan v. Connelly, 904 F.2d 112, 116 (1st Cir. 1990); *see also* Deal v. Spears, 980 F.2d 1153, 1157 (8th Cir. 1992).

76. 704 F.2d 577 (11th Cir. 1983).

77. *Id.* at 581.

78. *Id.*; *see also* Campiti v. Walonis, 611 F.2d 387, 394 (1st Cir. 1979) (refusing to imply consent to the interception of an inmate's telephone call despite defendant's arguments that the prisoner was generally aware that the prison routinely monitored inmate calls).

79. 704 F.2d at 581-82; *see also* Simmons v. Southwestern Bell Tel. Co., 452 F. Supp. 392, 396 (W.D. Okla. 1978) (implying consent when plaintiff made personal call on phone lines reserved for business use, even though he had previously been warned and other phones were available for personal use), *aff'd*, 611 F.2d 342 (10th Cir. 1979).

Jandak v. Village of Brookfield[80] represents another case that narrowly interpreted the consent exception. The plaintiff in *Jandak* was a private citizen who alleged that the Village of Brookfield had unlawfully intercepted her personal telephone conversation with a Brookfield police officer. After finding that neither party had given actual consent, the federal district court determined that the circumstances, including the department's routine monitoring of calls, established that the officer should have known that calls on the line were intercepted.[81] The court nonetheless rejected the consent defense by reasoning that Title III and its legislative history allowed consent to be "implied in fact" but did not allow consent to be "implied in law" based solely on a finding that one of the parties "reasonably should have known" of the monitoring.[82]

Following *Watkins* and *Jandak*, the Eighth Circuit in *Deal v. Spears*[83] further tested the limits of the consent exception as applied to employer telephone monitoring. The employer in *Deal* argued that employee consent could be implied because the employer had advised the employee that it might be forced to monitor phone conversations to reduce the number of personal calls. The employer also argued that a phone extension in the employer's home gave the employee actual notice of possible interception.[84] After reasoning that consent could not be "cavalierly implied," the court refused to find consent by emphasizing that the employer only informed the employee that it *might* begin monitoring the phone.[85] Furthermore, the court concluded that the employer must not have suspected that the employee was aware of the interception because the monitoring was designed to catch the employee admitting knowledge of a store burglary.[86] Regarding the extension phone, the court found no actual consent because the noise that notified the employee when someone picked up the extension phone was not triggered by the recording device installed by the employer.[87]

Although *Watkins*, *Jandak*, and *Deal* represent the strongest examples of judicial restraint in finding consent, their reasoning nevertheless implies that employers will escape liability if they publish a comprehen-

---

80. 520 F. Supp. 815 (N.D. Ill. 1981).
81. *Id.* at 820, 824-25.
82. *Id.* at 820 & n.5.
83. 980 F.2d 1153 (8th Cir. 1992).
84. *Id.* at 1156-57.
85. *Id.* at 1157 (quoting Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983)).
86. *Id.*
87. *Id.*

sive monitoring policy and abide by the its limits.[88] With such a policy, an employee's continued use of the E-mail network will presumably constitute, at a minimum, consent to employer interception of work-related messages and personal messages to the extent needed to determine whether the messages are personal or business in character.[89] An employer who publishes such a policy is thus only limited in that the scope of its intrusion must match the legitimate business interest justifying the invasion, and employers can expand the permissible scope simply by offering legitimate interests justifying broad monitoring policies.

Furthermore, policies that comport with *Watkins* and do not authorize full-content E-mail interception remain ineffective in protecting E-mail privacy because employees undoubtedly can never be certain to what extent employers actually peruse their communications. As long as employers are free to monitor employee communications, limiting the extent of the intrusion serves as mere damage control. Employers can still access, print, and scan even personal transmissions, thus vitiating the employee's limited consent.[90] In addition to amounting to self-regulation, such policies buttress the employer's argument that it is monitoring to protect its property. Specifically, the policies serve as evidence to the court that the employer's monitoring stems from a desire to protect its property and serve legitimate business purposes rather than from an offensive desire to invade its employees' privacy.[91]

Finally, consent remains only one of the exceptions to liability under the ECPA, and courts that do not find consent can nonetheless find the employer exempted from ECPA liability. For instance, despite its strong language against finding consent, the court in *Jandak* ultimately held that the reasons for recording the conversation and the fact that one of the parties "should have known" of the monitoring exempted the interception under the business-extension exception discussed below.[92]

---

88. *See* Baumhart, *supra* note 45, at 935; Barnett & Makar, *supra* note 17, at 737; John P. Furfaro & Maury B. Josephson, *Electronic Monitoring in the Workplace*, N.Y. L.J., July 6, 1990, at 32.

89. *See* Griffin, *supra* note 3, at 518.

90. *Id.*

91. Baumhart, *supra* note 45, at 935.

92. Jandak v. Village of Brookfield, 520 F. Supp. 815, 824-25 (N.D. Ill. 1981).

B. Provider Exception

The second primary exception frees system providers from general ECPA prohibitions on both access and disclosure. Specifically, the Act allows:

> [A]n officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service.[93]

The Act treats access to stored communications even more broadly, unconditionally exempting from liability "the person or entity providing a wire or electronic communications service."[94] Providers are also exempted in the portion governing the disclosure of stored communications. That section authorizes disclosure "(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination; (5) as may be necessarily incident to the rendition of the service or to the protection of the rights of property of the provider of that service."[95]

Many commentators, including the Electronic Mail Association, interpret this provider exception broadly to exclude most private employers from ECPA liability for perusing and disclosing employee E-mail communications that were transmitted through employer provided E-mail systems that use an employer's internal computer system.[96] This interpretation gives employers who provide their company E-mail networks almost "unfettered discretion" to read and disclose the contents

---

93. 18 U.S.C. § 2511(2)(a)(I) (1988).

94. 18 U.S.C. § 2701(c)(1) (1988).

95. 18 U.S.C. § 2702(b) (1988).

96. Kane, *supra* note 27, at 430; *see also* LaPlante, *supra* note 38, at 65; Baumhart, *supra* note 45, at 925. One commentator asserts that the ECPA does not apply to employers who monitor employee E-mail because the Act only addresses "third party" interception or accession. *See* Winters (1992), *supra* note 11, at 116-19. This characterization is imprecise because employers are "third parties" to employee-employee communications, and thus they must satisfy one of the three exceptions discussed in the text in order to be excepted from liability.

of even their employees' personal E-mail messages.[97] At least one commentator further believes that the exception exempts an employer who monitors E-mail transmitted through a public service E-mail provider if that employer uses the service only for internal communication.[98] These interpretations find support in dictum in *Flanagan v. Epson America, Inc.*,[99] an unreported California superior court decision, which is, at this writing, the only case to discuss employer E-mail monitoring under the ECPA. *Flanagan* primarily concerned the legality of E-mail interception under a California wiretapping statute, but the court analyzed in a footnote the applicability of the ECPA provider exception to the case and implied that the exception would have exempted the employer-provider from liability.[100]

Despite these arguments, many commentators warn employer-providers against relying too extensively on the provider exemption.[101] At a minimum, the exception does not appear to exempt employer interception if the employer merely provides for its employees standard E-mail service through a common carrier such as Prodigy, CompuServe, AT&T mail, SprintMail, or MCI mail.[102] Furthermore, if an employer

---

97. Hernandez, *supra* note 55, at 39-40.

98. Kane, *supra* note 27, at 430.

99. No. BC007036, slip op. at 5-6 n.1 (Cal. Super. Ct. Jan. 4, 1991).

100. *Id.* The court reasoned that "there simply is no ECPA violation if 'the person or entity providing a wire or electronic communications service' intentionally examines everything on the system." *Id.* (quoting Hernandez, *supra* note 55, at 39). *See infra* notes 370-72 and accompanying text; *see also* Nash, *Who Can Open E-mail?*, COMPUTERWORLD, Jan. 14, 1991, at 88.

101. Baumhart, *supra* note 45, at 925. At least one commentator suggests that the provider exception may not apply to employers who provide internal E-mail networks. He reaches his conclusion by reasoning that the use of the term "service" seems to indicate an external organization providing E-mail, especially given that the term "user" is defined as a "person *or entity* . . . who uses electronic mail." Droke, *supra* note 4, at 182 (analyzing 18 U.S.C. § 2510(13), (15) (1988)). This interpretation appears flawed because the ECPA does not specifically limit the term "provider" to mean common carriers and because some companies may still be providers of internal E-mail networks even though other companies may be properly considered users of networks provided by common carriers.

102. Baumhart, *supra* note 45, at 927. The ability of employers to access employee E-mail messages sent over a system not provided by the employer may be tested in Borland Int'l, Inc. v. Eubanks, No. 123059 (Cal. Super. Ct. filed Sept. 1992). *Borland* involves a case in which a software company retrieved stored, outgoing E-mail messages from a former employee in order to incriminate the employee for misappropriation of trade secrets. *See* Gina Smith, *Betrayal in Silicon Valley*, CAL. LAW., Apr. 1993, at 46; Stephen K. Yoder, *Grand Jury Charges Symantec Officers with Stealing Secrets from Borland*, WALL ST. J., Mar. 5, 1993, at B6; Stephen K. Yoder, *Silicon Valley Days: High-Tech Firm Cries Trade Secret Theft, Gets Scant Sympathy*, WALL ST. J., Oct. 8, 1992, at A1. The distinction between employer-provided E-mail networks and employer subscriptions to public service providers was also an issue in an unreported case involving an interception of E-mail transmitted via the Internet. *See* Baumhart, *supra* note 45, at 927 n.22 (citing Cameron v.

permits outsiders to use its internal E-mail system, and the amount of outside use becomes significant or the employer charges the outsiders to use its system, the employer might be considered a public E-mail provider, and as such would face special provisions regarding the disclosure of stored communications.[103]

Additional guidance in interpreting the provider exception may be found in courts' narrow interpretation of the common-carrier interception exception in the pre-ECPA context.[104] Congress essentially intended the original exception for common carriers to codify the principle established in *United States v. Beckley*,[105] in which a federal district court held that a telephone company may monitor its lines in order to prevent employee abuse.[106] Additionally, the Fifth Circuit's pre-ECPA analysis of the property protection exemption in *United States v. Clegg*[107] exemplifies the courts' unwillingness to read the exception broadly. In holding the telephone company's use of a pen register to be within the common-carrier exception, the *Clegg* court stressed that the register was used to protect long-distance abuse and did not intrude into the content of the telephone calls.[108]

Pre-ECPA courts also narrowly interpreted the alternative basis for the provider exemption that allows monitoring that is necessarily incidental to rendering the service. In fact, *Simmons v. Southwestern Bell Telephone Co.*[109] is the only case not otherwise explainable as a provider's inadvertent interception. *Simmons* involved the telephone company's interest in monitoring employee calls on telephones explicitly designated for business purposes, and the court concluded that the company's interest in maintaining the lines open for customer calls was incidental to the rendition of its services.[110] The court stressed, however, that the company would have "overstepped its limited privilege" if it had

---

Mentor Graphics, No. 716361 (Cal. Super. Ct. filed Nov. 7, 1991)).

103. *See* Kane, *supra* note 27, at 430-31 (interpreting 18 U.S.C. § 2702(a) (1988)).

104. Kane, *supra* note 27, at 431; Baumhart, *supra* note 45, at 931.

105. 259 F. Supp. 567, 571 (N.D. Ga. 1965).

106. S. REP. NO. 1097, 90th Cong., 1st Sess. (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2182.

107. 509 F.2d 605, 612-14 (5th Cir. 1975).

108. *Id.* at 612. The pen register only recorded the fact that a telephone call was made to a particular location at a particular time. *Id.* at 610. The Supreme Court subsequently held that the use of pen registers is not prohibited under Title III because pen registers do not intercept the contents of communications. United States v. New York Tel. Co., 434 U.S. 159, 166-68 (1977).

109. 452 F. Supp. 392 (W.D. Okla. 1978), *aff'd*, 611 F.2d 342 (10th Cir. 1979).

110. *Id.* at 396.

monitored calls on telephones available for personal use.[111] It thus appears that employer-providers may retain only a limited ability to monitor E-mail under the provider exception.

Given the absence of case law applying the provider exception to private employers who own and operate in-house E-mail networks, the ECPA legislative history is instructive in determining how courts should apply the exception. Portions of the legislative history support the position that Congress did not intend to prohibit employers from monitoring employee E-mail messages transmitted over employer-owned networks.[112] For instance, while the Senate report accompanying the passage of the ECPA noted the presence of employer-provided E-mail networks, the report did not mention whether the Act would affect such systems.[113] Furthermore, much of the testimony during the Senate hearing on the proposed legislation focused on the importance of corporate privacy, not the privacy of individual employees.[114]

However, accepting the position that the ECPA imposes no restrictions on employer-providers ignores the legislative history suggesting that such employers are not categorically excepted from the Act.[115] First, Congress explicitly stated that it desired to achieve parity in protecting personal communications without regard to the medium of transmission.[116] Interpreting the provider exception strictly would presumably result in protecting employees whose employers subscribe to an outside E-mail service while offering no protection to those employees whose employers provide their own in-house system.[117] Additionally, Congress specifically intended that pre-ECPA prohibitions should restrict employers who intercept telephone conversations of their employees; Congress may

---

111. *Id.*

112. Baumhart, *supra* note 45, at 926.

113. *Id.* at 926 (analyzing ECPA Legis. Hist., *supra* note 47, 1986 U.S.C.C.A.N. at 3562).

114. *Electronic Communications Privacy, 1985: Hearing on S. 1667 Before the Subcomm. on Patents, Copyrights, and Trademarks of the Senate Comm. on the Judiciary*, 99th Cong., 1st Sess. 40, 42 (1985) [hereinafter *Hearings on S. 1667*] (statement of Sen. Patrick J. Leahy (D-Vt.), co-sponsor); *id.* at 105 (statement of P. Michael Nugent, Board Member, Association of Data Processing Service Organizations ("ADAPSO")); *see also* Hernandez, *supra* note 55, at 40 ("ECPA 'goes right up to the water's edge [of employee privacy protection] but stops short' and to have included some privacy protection against employers in the corporate context 'would have killed the bill'" (quoting Jerry J. Berman, Chief Legislative Counsel, ACLU) (alteration in original)).

115. *See* Kane, *supra* note 27, at 431; Baumhart, *supra* note 45, at 925.

116. Baumhart, *supra* note 45, at 926; *see also* ECPA Legis. Hist., *supra* note 47, 1986 U.S.C.C.A.N. at 3559.

117. Baumhart, *supra* note 45, at 927.

therefore have seen no reason to extend ECPA prohibitions expressly to employer interceptions of electronic communications.[118] Moreover, Senate testimony noted that the ECPA was intended to cover all electronic communications, including those on employer-owned systems, because "electronic mail users obviously deserve privacy protection regardless of what type of entity runs their system."[119] Furthermore, the legislative history suggests that the main purpose of the provider exception was to allow providers to access the contents of stored electronic communications in order to back-up messages in case of system failure.[120] This emphasis on back-up protection is indicated in the ECPA's definition of electronic storage as being storage of electronic communications "for the purpose of back-up protection."[121]

In sum, the evidence appears contrary to the proposition that Congress intended the ECPA to leave employer access to and disclosure of employee E-mail communications unrestricted.[122] It seems likely that future applications of the provider exception will allow employer E-mail providers to retain at least the ability to access communications in order to minimize damages from system malfunction. Pre-ECPA cases and the legislative history, however, indicate that the provider exception may not apply when the employer goes beyond mere system maintenance and reads the content of E-mail messages. Because these kinds of actions will likely form the heart of employee privacy claims,[123] courts will be forced to address the scope of the exception and the limits to acceptable employer-provider activities. The extent to which employer-providers are exempt under the provider exception is not yet certain.[124] *Flanagan*

---

118. *Id.*

119. *Hearings on S. 1667*, *supra* note 115, at 146 (testimony of Jerry J. Berman, Chief Legislative Counsel, ACLU); *id.* at 99-100 (statement of Philip M. Walker, Vice-Chair, Electronic Mail Association). The Senate Subcommittee chair overseeing Senate ECPA hearings also stated that, absent "positive signals" to the contrary, E-mail users "generally [would have] an expectation of privacy." *Id.* at 147 (testimony of Sen. Charles Mathias, co-sponsor, S. 1667); *see also id.* at 151 (statement of Sen. Charles Mathias, Mark-up Session on S. 2575, Aug. 12, 1986) (noting that the interest would be legally enforceable).

120. Baumhart, *supra* note 45, at 928 (citing H. REP. NO. 647, 99th Cong., 2d Sess. 22 n.34 (1986)) ("E-mail systems are designed to provide access to contents and copies of messages in case of system failure. Messages are electronically generated and not normally accessed by the E-mail provider.").

121. 18 U.S.C. § 2510(17)(B) (1988).

122. *See* Baumhart, *supra* note 45, at 928.

123. *See, e.g.*, Bourke v. Nissan Motor Corp., No. B068705 (Cal. Ct. App. July 26, 1993) (employees claimed wrongful termination and invasion of privacy after the employer reviewed various personal E-mail messages from the plaintiffs to other employees).

124. *See, e.g.*, Kane, *supra* note 27, at 430-31; Baumhart, *supra* note 45, at 929.

remains the only case to address the applicability of the provider exception, and there the court implied that the employer would be exempted.[125] Thus, given the textually broad scope of the provider exception and the current emphasis on employer business interests, employee E-mail messages transmitted over an employer-provided system remain exposed to potential lawful interception.

C. Business-Extension Exception

The final important exception to ECPA liability is known as the "business-extension," "business use," or "ordinary course of business" exception.[126] Actions brought under the ECPA require the plaintiff to demonstrate that the alleged violator used an "electronic, mechanical or other device" to intercept the communications at issue.[127] The business-extension exception excludes from the definition of *electronic device*:

> [A]ny telephone or telegraph instrument, equipment or facility, or component thereof, I) furnished to the subscriber or user in the ordinary course of business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such services and used in the ordinary course of its business.[128]

In contrast to the legislative history of the provider exception, the extensive Title III legislative history provides virtually no guidance in ascertaining what Congress intended by the business-extension exception.[129] Case law, however, remains helpful because courts have extensively applied the business-extension exception to telephone communications and other analogous contexts, even though they have not

---

125. Flanagan v. Epson Am., Inc., No. BC007036, slip op. at 5-6 n.1 (Cal. Super. Ct. Jan. 4, 1991).

126. Michael Traynor, *Computer E-mail Privacy Issues Unresolved,* NAT'L L.J., Jan. 31, 1994, at S2; Barnett & Makar, *supra* note 17, at 725.

127. 18 U.S.C. § 2510(4) (1988); *see also* Barnett & Makar, *supra* note 17, at 725.

128. 18 U.S.C. § 2510(5)(a) (1988).

129. *See* Briggs v. American Air Filter Co., 630 F.2d 414, 418 (5th Cir. 1980) (citing Simpson v. Simpson, 490 F.2d 803 (5th Cir. 1974)).

yet applied the exception in cases of E-mail interception.[130] In fact, this exception accounts for most of the litigation brought under the ECPA.[131]

In analyzing such applications, courts usually take one of two approaches to determine whether the employer monitoring is lawful under the Act. The context approach emphasizes the employer's perspective[132] by examining the propriety of the circumstances surrounding the workplace monitoring.[133] In contrast, the content approach asks whether the employer has a business interest in interception by evaluating whether the particular communication was business or personal in character.[134]

1. The Context Approach

Courts applying the context approach concentrate on particular factors such as whether the employer had a legitimate business interest justifying the interception and whether employees were notified that the employer may intercept their communications.[135] Under this approach, employers generally escape liability if they satisfy a checklist of objective considerations.[136] The approach appears flawed at the outset because it analyzes contextual cues that affect the employees' subjective expectation of privacy even though the ECPA protects electronic communications regardless of whether the plaintiff demonstrates such an expectation.[137] Courts may justify their analysis, however, by emphasizing that the business-extension exception is actually an exception to the definition of "electronic device," and not to the definition of "electronic communication."[138]

The principal case applying the context approach is *United States v. Harpel*.[139] In holding the interception illegal, the Tenth Circuit established a minimum standard for workplace monitoring as including employer authorization and adequate employee notice—in other words,

130. *See* Winters (1992), *supra* note 11, at 118. Neither Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994), nor *Flanagan* discussed the exception. *See supra* notes 72-73 and *infra* notes 351-59 and accompanying text.

131. Griffin, *supra* note 3, at 514.

132. *Id.* at 515.

133. Barnett & Makar, *supra* note 17, at 727-28.

134. *Id.* at 727-28, 730; Griffin, *supra* note 3, at 515-16.

135. Barnett & Makar, *supra* note 17, at 728.

136. *Id.*

137. *Id.*; *see also* 18 U.S.C. § 2510(12) (1988) (definition of "electronic communication").

138. *See* Barnett & Makar, *supra* note 17, at 728.

139. 493 F.2d 346 (10th Cir. 1974).

consent.[140] Courts applying the context approach have also scrutinized the employer's business justifications for the interception. For instance, in *James v. Newspaper Agency Corp.*, an employer decided to install a monitoring device on the telephones used by employees dealing with the public.[141] The employer reasoned that the device would provide some protection for employees against abusive calls and would enable supervisors to provide training and instruction to the employees. The employer informed its employees, no employee protested, and the telephone company completed the installation. From these facts, the court found the employer's actions to "come[] squarely" within the business-extension exception.[142] The court distinguished *Harpel* by emphasizing that the installation in *James* was fully disclosed to employees and was for a legitimate business purpose.[143]

The Eighth Circuit in *Deal v. Spears* bifurcated the exception into two elements, requiring: (1) the interception equipment to be provided to the subscriber by the phone company or connected by the subscriber to the phone line; and (2) the interception to be in the ordinary course of business.[144] In addressing the first element, the court disagreed with other circuit court holdings, concluding that the recording device used by the employer to monitor the employee calls, not the extension telephone, was the critical intercepting device. The court thus reasoned that the device was not covered by the exception because it was purchased by the employer at Radio Shack, and was not provided by the telephone company.[145]

Although this first conclusion removed the employer's monitoring from the exception, the court went on to conclude that the interception was also not in the ordinary course of business. The court acknowledged that the employer's interest in catching a store burglar legitimized some telephone monitoring.[146] The court, however, determined that this interest justified neither the employer's recording twenty-two hours of calls, the vast majority of which were personal, nor the employer's listening to them without regard to its business interest in the calls. After citing the

---

140. *See id.* at 351; Barnett & Makar, *supra* note 17, at 728.

141. 591 F.2d 579, 581 (10th Cir. 1979).

142. *Id.*

143. *James*, 591 F.2d at 582; *see* Simmons v. Southwestern Bell Tel. Co., 452 F. Supp. 392, 396 (W.D. Okla. 1978) (holding interception to be lawful under the business-extension exception), *aff'd*, 611 F.2d 342 (10th Cir. 1979).

144. 980 F.2d 1153, 1157 (8th. Cir. 1992).

145. *Id.* at 1158.

146. *Id.*

scope limitations enunciated in *Watkins v. L.M. Berry & Co.*,[147] the court concluded that the interception was "well beyond the boundaries of the ordinary course of business."[148]

The case that most recently addressed the business-extension exception applied the context approach. The Fourth Circuit in *Sanders v. Robert Bosch Corp.*[149] explicitly adopted the two-prong test established by the Eighth Circuit in *Deal*. Applying the first prong, the court held that the "voice logger" recording device was not within the exception because it was not a "telephone instrument" that "further[ed] the [employer's] communication system."[150] Regarding the second prong, the court rejected the employer's argument that the voice logger, which surreptitiously recorded all conversations over certain phone lines, was used in the ordinary course of business because the employer feared bomb threats. The court reasoned that the evidence of bomb threats was scant and that the employer's rationale did not justify the employer's failure to inform the nonsupervisory employees that all calls on certain lines were recorded twenty-four hours a day.[151]

2. *The Content Approach*

Unlike the context approach, the content approach emphasizes the content of the intercepted communication and reasons that employers can lawfully intercept "business" communications but not "personal" communications.[152] In addition to defining the limits of the consent exception, *Watkins* is the seminal case to apply the content approach to the business-extension exception. In *Watkins*, the Eleventh Circuit held that the employer must show that the *particular* interception at issue was in the ordinary course of business; therefore, the employer must

---

147. 704 F.2d 577 (11th Cir. 1983).

148. *Deal*, 980 F.2d at 1158; *see also* People v. Otto, 9 Cal. Rptr. 2d 596, 607-08 n.14 (1992) (suggesting that employer eavesdropping must be limited to a particular purpose, time, and place to be protected by the business-extension exception, and that the exception does not cover a general practice of "surreptitious monitoring"), *cert. denied*, 113 S. Ct. 414 (1992).

149. 38 F.3d 736 (4th Cir. 1994).

150. *Id.* at 740-41 & n.9. The court noted that the fact that the recording device was not a "telephone instrument" under the ECPA removed the device from the exception regardless of whether the telephone company or the employer had furnished the device.

151. *Id.* at 740-41. One judge dissented from the panel's determination that the recording was not included within the business-extension exception. *Id.* at 743-47 (Widener, J., dissenting).

152. *See* Barnett & Makar, *supra* note 17, at 730; Baumhart, *supra* note 45, at 931.

demonstrate a "legal interest" in the subject matter of the intercepted call. The court thus concluded that employer monitoring of employee personal calls is never "in the ordinary course of business . . . except to the extent necessary to guard against the unauthorized use of the telephone or determine whether a call is personal or not."[153] The court added that in order to remain within the exception, a manager must cease listening in on an employee call once the call turns personal.[154] In *Watkins*, the employer had monitored a discussion between two employees concerning a job interview one of them had undergone at another company. Although the court noted that the conversation may have been of interest to the employer, it concluded that the conversation was not in the employer's legal interest because it was "neither in pursuit nor to the legal detriment of [the employer's] business."[155] The court further reasoned that "the ordinary course of business exception cannot be expanded to mean anything that interests a company."[156]

In contrast to *Watkins*, the Fifth Circuit in *Briggs v. American Air Filter Co.*[157] liberally construed the employer's legal interest in telephone monitoring, explicitly rejecting the idea that non-consensual interception is never allowed within the business-extension exception. In holding the employer not liable for the interception, the Fifth Circuit emphasized that the employer had a legitimate suspicion that its interests were at stake and that the employer limited the interception in time and scope to intercepting the business portion of the call for the particular business purpose.[158] The court stressed that it might have decided the case differently had the employer used the extension phone to monitor a personal portion of any conversation or had the employer engaged in a general practice of surreptitious monitoring.[159]

---

153. *Watkins*, 704 F.2d at 582-83.

154. *Id.* at 584. The court noted that other cases were reasonable in allowing interception of ten to fifteen seconds but that one case allowing a three to five minute interception was troubling. *Id.* at 584-85.

155. *Id.* at 582.

156. *Id.* Following *Watkins*, the court in Abel v. Bonfanti, 625 F. Supp. 263, 270 (S.D.N.Y. 1985), reasoned that a personal call cannot be intercepted in the ordinary course of business. *See also* Awbrey v. Great Atl. & Pac. Tea Co., 505 F. Supp. 604, 610 (N.D. Ga. 1980) (declining to dismiss a claim of unlawful wiretapping based on the employer's monitoring of business telephones from which employees made personal calls).

157. 630 F.2d 414, 419 (5th Cir. 1980).

158. *Id.* at 420.

159. *Id.* at 420 & n.8.

The personal-business distinction in *Briggs* was similarly applied in *Epps v. St. Mary's Hospital of Athens, Inc.*[160] *Epps* involved the monitoring of a telephone conversation between co-employees concerning "scurrilous remarks" about supervisory employees.[161] The employees whose conversation had been intercepted urged a contextual approach by asserting that the employer had not followed company policy in conducting the interception.[162] In adopting the content approach, the Eleventh Circuit reasoned that the call was not personal because it occurred between co-employees during office hours over a specialized extension, and because it involved remarks about supervisory employees in their capacities as supervisors.[163] The court stated that "[c]ertainly the potential contamination of a working environment is a matter in which the employer has a legal interest."[164] The court thus concluded that the monitoring fell within the business-extension exception.[165]

3. *Application of the Two Approaches to E-mail Monitoring*

The application of the business-extension exception to E-mail communications will vary depending on whether courts adopt a contextual or content-based approach. Specifically, courts applying the context approach would examine relevant factors within the work environment to determine whether the interception was excepted. Following *James*, courts would concentrate on whether the employer had notified the employees of possible E-mail monitoring. In contrast, courts using the content analysis would focus on the subject matter of the intercepted messages. Presumably, by applying *Watkins*, courts would allow the interception of work-related E-mail messages but would allow the

---

160. 802 F.2d 412, 416-17 (11th Cir. 1986).

161. *Id.* at 417. The employees argued that the double reel recording device, which recorded the calls, was not excepted because it was not an intercepting device furnished by the telephone service. *Id.* at 415. The court, however, did not accept their argument and reasoned that the dispatch console was the intercepting device because the console actually intercepted the call while the recorder recorded it. *Id. But see* Deal v. Spears, 980 F.2d 1153, 1158 (8th Cir. 1992) (holding that the recording device, not the telephone extension, was the critical intercepting device under the exception); Sanders v. Robert Bosch Corp., 38 F.3d 736, 740 n.3 (4th Cir. 1994) (following *Deal*).

162. *Epps*, 802 F.2d at 416.

163. *Id.* at 417.

164. *Id.*

165. *Id.*; *see also* Burnett v. State of Texas, 789 S.W.2d 376 (Tex. Ct. App. 1990) (holding that business-extension exception protected employer's use of an extension phone to intercept the call of an employee who was being investigated for suspected theft of the employer's property).

interception of personal communications only to the extent necessary to determine whether the communications are business or personal.

Regardless of these differences, both approaches nevertheless inadequately protect employee E-mail privacy in certain circumstances. The context approach is flawed in that it provides the employee with no protection of even personal E-mail messages when the employer satisfies certain criteria. An employer could therefore access E-mail indiscriminately as long as its actions were authorized by proper employee notification and the monitoring did not violate other legal interests.

The dissent in *Epps* highlights the flaws in the content approach. First, as the dissent reasoned, focusing on the content of the communication is misplaced; the real issue should be the behavior and legitimate interests of the employer.[166] Second, using the content of an employee's conversation to justify an employer intrusion is problematic because the employer should have adequate justification and authorization *at the time* it invades employee privacy.[167] Because the business or personal nature of most communications cannot be determined without actually intercepting the content of messages, this approach seemingly excepts all E-mail interceptions as long as the interception is limited to determining the business or personal nature of the message.[168] The third problem in the content approach concerns how courts should determine whether the content of a particular communication is "business" or "personal."[169] Courts offer differing approaches for locating the borderline between business and personal calls, although they generally reason that a business call must be "reasonably related to a business purpose."[170] At best, the distinction between business and personal remains nebulous.[171]

The second problem in the content approach might be avoided when applied to E-mail because the subject matter of E-mail communications, unlike telephone conversations, can be determined without accessing the actual content of the messages. E-mail messages are customarily formatted in a style similar to written memoranda by including separate

---

166. *Epps*, 802 F.2d at 417 (Kravitch, J., dissenting).

167. *See id.* at 418 (Kravitch, J., dissenting).

168. *See* Fitzpatrick (1991), *supra* note 8, at 39. For instance, because the content of the communication was deemed to have been in the employer's interest, the court in *Epps* allowed the interception even though notice and other important contextual factors were absent. *Epps*, 802 F.2d at 417.

169. Barnett & Makar, *supra* note 17, at 732.

170. Briggs v. American Air Filter Co., 630 F.2d 414, 420 (5th Cir. 1980); James v. Newspaper Agency Co., 591 F.2d 579, 581-82 (10th Cir. 1979).

171. Barnett & Makar, *supra* note 17, at 736.

heading and transactional information in which the sender briefly describes the content of the E-mail message.[172] Commentators thus suggest that the content limitation may be effective if employers institute an interception program that searches only the transactional information of employee E-mail messages.[173] Although employers could utilize these headings to avoid intercepting messages considered personal, this solution may not be feasible because employers would presumably object to relying on headings that employees themselves compose. Employer skepticism would likely persist even though most employees have disincentives to mislabel their messages intentionally.[174] Moreover, utilizing the headings would not completely end judicial difficulties in demarcating the line between business and personal communications because the battle would simply be transferred from the message content to the subject description in the heading of each E-mail message.

Employers could also search E-mail files for specific key words or phrases to identify messages that compromise the employer's legal interests.[175] Such key word searches have an advantage over searching the transactional information in that key word searches can search the actual content of the E-mail communications. This solution, however, ultimately remains insufficient for the majority of employer interests because inappropriate messages are almost always unidentifiable by certain key words or phrases.

Interestingly, neither approach clearly suggests what device will constitute the "electronic device" intercepting E-mail for the purpose of determining whether the business-extension exception applies in a particular context. Employers most often intercept E-mail messages from in-house central computers, which are necessary in "the ordinary course of business" to route incoming and outgoing transmissions. Many of these computers systematically record and copy the transmitted messages in order to minimize losses resulting from system failure. Given the fact that the central computer both routes and records messages, courts will likely uniformly brand the central computer the intercepting device and

---

172. *See, e.g.*, Baumhart, *supra* note 45, at 933.

173. Griffin, *supra* note 3, at 518-19 (citing Caldwell, *supra* note 22, at 34)).

174. Mislabelling would cause the employee to appear unproductive if the employer monitors E-mail to gauge employee productivity.

175. In Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 463 (5th Cir. 1994), the court noted that the risk of accessing unrelated stored electronic communications can be minimized through key word searches. *See supra* notes 72-73 and accompanying text.

will avoid the discrepancy between *Deal* and *Sanders* on the one hand and *Epps* on the other as to whether the recording instrument or the actual extension phone is the intercepting device.

Regardless of how the courts apply the specifics of the exception, each approach involves an implicit balancing of the reasonableness of the employee's privacy expectations against the legitimacy of the employer's business justifications for monitoring. Courts determine the reasonableness of the employee's expectations in the context approach by analyzing the employer's notification procedures. They decide the legitimacy of the employer's interest in the content approach by analyzing the purposes behind the monitoring and whether the content of the communication is reasonably related to the proffered purposes.[176] The above cases suggest the importance of the employer's proffered business justifications. While legitimate business interests will not justify a general practice of extensive E-mail content monitoring, the scope of the acceptable monitoring generally corresponds to the employer's business interests.[177] Ultimately, the employer need only produce a legitimate business interest to match the level of E-mail monitoring it desires.[178]

The balancing process implicit in both the content and context approaches parallels the balancing of interests and limitation of scope present in both tort and Fourth Amendment privacy analysis.[179] Presumably, courts will continue to utilize this pervasive balancing as they apply existing laws to unauthorized interceptions and accessions of E-mail. Although the above limitations may appear to restrict invasive employer monitoring effectively, the limitations in reality only extend their privacy protection to the point at which the employer can proffer no sufficient business interest to justify the E-mail monitoring. Indeed, satisfying such a standard may be rather easy given that employers can

---

176. *See* Barnett & Makar, *supra* note 17, at 756-57. For instance, courts likely will tolerate employer content monitoring when it is necessary to prevent computer crime or protect trade secrets. *See* Baumhart, *supra* note 45, at 933-34. One commentator also suggests that retrieving lost messages, helping employees effectively utilize the E-mail system, and determining whether employee gossip hurts workplace morale all are interests that would justify E-mail monitoring. Griffin, *supra* note 3, at 517.

177. *See, e.g.*, Deal v. Spears, 980 F.2d 1153, 1158 (8th Cir. 1992) (holding that the employer's interest did not justify the pervasive extent of the invasion); Briggs v. American Air Filter Co., 630 F.2d 414, 420 n.9 (5th Cir. 1980) ("A general practice of surreptitious monitoring would be more intrusive on employee's privacy than monitoring limited to specific occasions.").

178. Griffin, *supra* note 3, at 517.

179. *See infra* notes 182-283 and accompanying text.

always argue that they have legitimate interests in workplace productivity, efficiency, and quality control.[180]

II. STATE LAW CLAIMS

Despite the existence of federal laws protecting privacy, an employee's general right to privacy is largely an issue of state law.[181] State laws are often more expansive than federal laws,[182] leading some commentators to suggest that state law represents the best existing source for protecting private employees from E-mail interception by their employers.[183]

A. Tort Law

The traditional legal stronghold for the protection of non-governmental employees' privacy has been the common law tort system.[184] In a seminal 1890 law review article, Samuel D. Warren and Louis D. Brandeis observed a development in tort law that was expanding protection beyond traditional property rights to what they expressed as "inviolate personality"—"the right of determining to what extent [an individual's] thoughts, sentiments, and emotions shall be communicated to others."[185] Since their article, workplace privacy has developed as a protected interest in virtually all states under the state common law tort of invasion of privacy.[186]

---

180. *See* Lois R. Witt, *Terminally Nosy: Are Employers Free to Access Our Electronic Mail?*, 96 DICK. L. REV. 545, 552-53 (1992); Semore v. Pool, 266 Cal. Rptr. 280, 287 (Cal. Ct. App. 1990).

181. *See* Katz v. United States, 389 U.S. 347, 350-51 (1967).

182. *See* Barnett & Makar, *supra* note 17, at 719 (noting the example of stringent Florida privacy laws).

183. *See, e.g.*, Winters (1992), *supra* note 11, at 119.

184. *See* Cavico, *supra* note 9, at 1266.

185. Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 205, 198 (1890).

186. Fitzpatrick (1992), *supra* note 3, at 1175; *see also* RESTATEMENT (SECOND) OF TORTS § 652A app. reporter's note (1989 & Supp. 1990). Some states have passed statutes that essentially adopt the common law right of privacy. *See* Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 228 (1992).

1. Intrusion Upon Seclusion

A scheme of four distinct torts protects the right to privacy: (1) unreasonable intrusion upon the seclusion of another; (2) misappropriation of another's name or likeness; (3) unreasonable publicity given to another's private life; and (4) publicity that unreasonably places another in a false light before the public.[187] Each tort recognizes a "substantial zone of freedom,"[188] where an individual has the right "to be let alone."[189] The one most relevant to E-mail interception or accession is the "unreasonable intrusion upon the seclusion of another" tort.[190] This tort holds that "one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[191]

Because the invasion may be nonphysical, the tort protects one against electronic eavesdropping.[192] Liability under this tort does not require that private, personal information be acquired in the invasion,[193] especially where an employer's intrusion is abnormal in character.[194] Furthermore,

---

187. RESTATEMENT (SECOND) OF TORTS § 652A (1977); *see also* W. PAGE KEETON, ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 117, at 851 (5th ed. 1984).

188. *See* Young v. Jackson, 572 So. 2d 378, 381 (Miss. 1990).

189. KEETON ET AL., *supra* note 188, § 117, at 849, 851 (quoting COOLEY, TORTS 29 (2d ed. 1888)).

190. *See* Griffin, *supra* note 3, at 503-04. This statement presumes that the information accessed in the interception is not disclosed. If the information is publicized, the employee might maintain an action under the tort for unreasonable publicity given to another's private life. *See* Baumhart, *supra* note 45, at 947; Jenero & Mapes-Riordan, *supra* note 5, at 81. For a case addressing this second tort, see Bratt v. IBM Corp., 785 F.2d 352, 360 (1st Cir. 1986) (reasoning that the test for invasion of privacy is "whether the substantiality of the intrusion on the employee's privacy which results from the disclosure outweighs the employer's legitimate business interest in obtaining and publishing the information").

191. RESTATEMENT (SECOND) OF TORTS § 652B (1977); *see also* Leggett v. First Interstate Bank, N.A., 739 P.2d 1083, 1086 (Or. Ct. App. 1987) (citing Oliver v. Pacific N.W. Bell Tel. Co., 632 P.2d 1295, 1298 (Or. Ct. App. 1981)); KEETON ET AL., *supra* note 188, at 854-55.

192. *See, e.g.*, Roach v. Harper, 105 S.E.2d 564, 568 (W. Va. 1958); Rhodes v. Graham, 37 S.W.2d 46, 47 (Ky. 1931); RESTATEMENT (SECOND) OF TORTS § 652B cmt. b at 378-79 (1977).

193. Phillips v. Smalley Maintenance Serv., Inc., 711 F.2d 1524, 1534 (11th Cir. 1983) (holding that acquisition of private information was not necessary in order for an intrusion upon seclusion to occur); Phillips v. Smalley Maintenance Serv., Inc., 435 So. 2d 705, 709 (Ala. 1983) (same).

194. KEETON ET AL., *supra* note 188, § 117, at 856 (noting that abnormal means for gaining access to information, such as wiretapping, would be actionable as an invasion of privacy regardless of purpose); *see* Comeaux v. Brown & Williamson Tobacco Co., 915 F.2d 1264, 1275 (9th Cir. 1990) (reasoning that invasion of privacy is available to redress

the intrusion need not be surreptitious,[195] and the improperly obtained information need not be publicized or used by the employer.[196] Express or implied consent is one defense to liability, yet the defendant's good faith belief that consent has been given is normally not a defense, although such a belief may mitigate punitive damages.[197]

The elements of the tort are similar to the standards used in determining a Fourth Amendment claim in the public sector.[198] For behavior to be actionable, the employee-plaintiff must prove the employer committed a highly offensive intentional intrusion into a private matter.[199] Courts generally consider electronic surveillance, such as telephone monitoring, an "intrusion" sufficient to establish the first element of a prima facie case.[200] In deciding whether the intrusion is into a private matter, courts require not only that the employee have a subjective expectation of privacy but also that the expectation be objectively reasonable.[201] Finally,

---

harm caused by "the use of *outrageous investigative methods*" (emphasis added)).

195. *See, e.g., Phillips*, 711 F.2d at 1535 (rejecting the argument that a claim for invasion of privacy was barred because the intrusive actions occurred "out in the open"); Bennett v. Norban, 151 A.2d 476, 478-79 (Pa. 1959) (finding a violation of privacy when store manager stopped plaintiff and publicly searched her pockets on suspicion of shoplifting, despite the absence of clandestine conduct involved in the search).

196. Borse v. Piece Goods Shop, Inc., 963 F.2d 611, 621 (3d Cir. 1992); *Phillips*, 711 F.2d at 1535; RESTATEMENT (SECOND) OF TORTS § 652B cmt. a at 378 (1977).

197. KEETON ET AL., *supra* note 188, § 117, at 867-68; *see also* Griffin, *supra* note 3, at 505.

198. In order to prove a Fourth Amendment violation, the claimant must exhibit an actual, subjective expectation of privacy, and the expectation must be one that society is prepared to regard as reasonable. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The subjective test focuses on the means the claimant has used to protect his or her privacy. Kane, *supra* note 27, at 422. *See infra* notes 209-20 and accompanying text (analyzing the "objectively reasonable" prong of the privacy test).

199. Jenero & Mapes-Riordan, *supra* note 5, at 81; *see* Lee, *supra* note 25, at 162-63 (noting that courts consider whether the intrusion was intentional). Some courts have added a fourth prong requiring that the plaintiff prove "anguish and suffering" as a result of the intrusion. *See, e.g.*, Hoth v. American States Ins. Co., 735 F. Supp. 290, 293 (N.D. Ill. 1990).

200. Jenero & Mapes-Riordan, *supra* note 5, at 81. In most instances, courts consider the means and purpose concurrently when determining whether an employer interception or accession is an intrusion constituting an actionable invasion of privacy. Courts often utilize this analysis to allow employee drug testing. *See, e.g.*, Luedtke v. Nabors Alaska Drilling, Inc., 768 P.2d 1123, 1136 (Alaska 1989); Jennings v. Minco Tech. Labs, Inc. 765 S.W.2d 497, 499 (Tex. Ct. App. 1989). Using this analysis, one court allowed an employer to observe an employee at home through an open window with the assistance of a high-power camera lens. Saldana v. Kelsey-Hayes Co., 443 N.W.2d 382, 384 (Mich. Ct. App. 1989).

201. *See* Droke, *supra* note 4, at 184-86; Barnett & Makar, *supra* note 17, at 741 (citing *Katz*, 389 U.S. at 361 (Harlan, J., concurring)); *see also* Hill v. National Collegiate Athletic Ass'n, 865 P.2d 633, 648 (Cal. 1994). Thus, even if employees can successfully establish that their E-mail messages were private and not the employer's property, they still must prove that their expectations of privacy were reasonable and not outweighed by

in determining the offensiveness of an intrusion, courts examine "the degree of intrusion, the context, conduct, and circumstances surrounding the intrusion, as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded."[202]

As a general rule, an employee enjoys a protectable privacy interest in those items that the employee owns or exclusively uses, or items of such a nature that the employee has a reasonable expectation of privacy.[203] In applying this analysis to E-mail, the particular circumstances of the employment setting remain critical. Normally, an employee creates an individual password to access the employee's own messages. Such a password undoubtedly encourages a subjective belief among employees that their E-mail messages are private,[204] given that employees are often unaware that their employer retains the ability to override the password and access their E-mail.[205] It is thus understandable that most of the litigation concerning privacy expectations has concerned whether the expectation is objectively reasonable, since employees have easily demonstrated subjective privacy expectations.[206] This emphasis on the objective prong will continue as employers seek to alter the objective reasonableness of subjective expectations by modifying the extrinsic factors of the work environment.[207]

Many factors and policies of the particular workplace affect whether the privacy expectation is reasonable.[208] For instance, employees may have a greater expectation of privacy when their E-mail correspondence at work is transmitted over a common carrier than when the messages are

---

employer interests. *Cf.* Simmons v. Southwestern Bell Tel. Co., 452 F. Supp. 392, 396 (W.D. Okla. 1978) (finding no reasonable expectation of privacy in personal calls made with a telephone on which personal calls were prohibited), *aff'd*, 611 F.2d 342 (10th Cir. 1979).

202. Miller v. NBC, 232 Cal. Rptr. 668, 679 (Ct. App. 1986).

203. Witt, *supra* note 181, at 560-61.

204. *See id.* at 555, 561 (arguing that, with the password, an employee's E-mail files become the exclusive property of the employee, in a relationship similar to that between an employee and a filing cabinet or a file marked "personal"); Droke, *supra* note 4, at 185; Kane, *supra* note 27, at 439; Note, *supra* note 3, at 1909-10.

205. Heredia, *supra* note 3, at 331 (attributing employees' belief in the privacy of their communications to their lack of knowledge concerning how access to E-mail systems works).

206. *See* Droke, *supra* note 4, at 184-86.

207. Barnett & Makar, *supra* note 17, at 742 (1988).

208. *See* Witt, *supra* note 181, at 565. *See generally* Hill v. National Collegiate Athletic Ass'n, 865 P.2d 633, 655 (Cal. 1994) (discussing how physical settings and practices affect privacy expectations).

transmitted over an employer-owned computer system.[209] Privacy expectations may also be greater with systems that allow employees to create and modify personal passwords at any time, as opposed to systems that use employer-provided passwords.[210] Furthermore, employee notification is important because, as under the ECPA analysis, courts may imply consent to E-mail monitoring when employers provide notice or when the employees are aware that monitoring can occur.[211] Additional factors include the degree of employer access to the E-mail system and the type of information usually transmitted over the system.[212] Finally, courts may determine the reasonableness of the privacy expectation by analyzing the means an employer uses to obtain the information. Because this final consideration also affects whether the intrusion itself was reasonable,[213] courts that find a reasonable expectation of privacy will likely also find the invasion to be highly offensive to a reasonable person.[214]

Since courts have historically held that business interests can justify even extremely invasive conduct,[215] employees maintain few privacy interests that cannot be overridden by strong employer interests or by customarily intrusive business practices. In fact, commentators have recognized that employers "need only assert some business interest to seek information about virtually any employee action or utterance"[216] and that the concept of "'business interest' creates almost a legal safe haven for employers who choose to monitor employee E-mail messages."[217]

---

209. *See* Droke, *supra* note 4, at 184-85.

210. *Id.* Employees' work environment may also affect their technical expertise, which in turn affects their privacy expectation. For instance, employees in a high-technology firm may be more aware of the potential for system interception than employees in a general business environment. *Id.* at 185.

211. Heredia, *supra* note 3, at 330, 334; Droke, *supra* note 4, at 184-85; Barnett & Makar, *supra* note 17, at 742. Employers retain complete control over the degree of notice, but they may not provide detailed notice in order to intercept more revealing information. Droke, *supra* note 4, at 185.

212. Droke, *supra* note 4, at 184-85.

213. KEETON ET AL., *supra* note 188, § 117, at 856; *see also* Droke, *supra* note 4, at 186.

214. Droke, *supra* note 4, at 186.

215. *See, e.g.*, Saldana v. Kelsey-Hayes Co., 443 N.W.2d 382, 384 (Mich. Ct. App. 1989) (concluding that employer's legitimate business interest in investigating employee's claim of work-related injury outweighed employee's privacy interest in not being monitored in his home).

216. Griffin, *supra* note 3, at 509.

217. *Id.* at 526-27. For example, an employer who monitors telephone calls in an effort to ensure quality control and who provides employee notice of such monitoring satisfies the reasonable conduct requirement. Simmons v. Southwestern Bell Tel. Co., 452

The critical issues in determining employer tort liability for E-mail interception are thus whether employees have a reasonable expectation of privacy in their E-mail correspondence[218] and whether their employer offers legitimate business justifications for the intrusion.[219]

2. *Case Law Analysis*

a. *Common law cases*

Courts have not yet widely applied tort doctrines to employer interception and accession of employee E-mail messages.[220] The only case to date to do so is *Bourke v. Nissan Motor Corp.*,[221] an unpublished 1993 California case, in which the employer intercepted numerous personal E-mail messages, including some of a sexual nature, from the plaintiffs to other employees. In rejecting the employees' claims, the court held, as a matter of law, that the plaintiffs had no reasonable expectation of privacy in their E-mail messages because they had signed a user waiver form stating that "it is company policy that employees and contractors restrict their use of company-owned computer hardware and software to company business." Additionally, the court determined that the plaintiffs had no reasonable expectation of privacy because many months before their terminations they learned that their E-mail messages were periodically read by employees other than the intended recipients. Although the plaintiffs further argued that they had a privacy expectation because they were given passwords to access the system and were told to safeguard their passwords, the court held that such a claim did not raise

---

F. Supp. 392, 394 (W.D. Okla. 1978), *aff'd*, 611 F.2d 342 (10th Cir. 1979).

218. Droke, *supra* note 4, at 184.

219. *See* Linowes & Spencer, *supra* note 2, at 593; *see also* J. Clark Kelso, *California's Constitutional Right to Privacy*, 19 PEPP. L. REV. 327, 376 (1992).

220. Cavico, *supra* note 9, at 1328.

221. No. B068705 (Cal. Ct. App. July 26, 1993); *see* Traynor, *supra* note 127, at S3. In addition to the California case, Washington Fed'n of State Employees v. Department of Labor & Indus., No. 90 2 02130 8 (Wash. Super. Ct. filed Sept. 10, 1990), is an E-mail privacy case in the state of Washington affecting public employees. The Washington case differs significantly from the California case in that it involves state action. *See* Griffin, *supra* note 3, at 494 n.3. Cubby v. CompuServe, 776 F. Supp. 135 (S.D.N.Y. 1991), another case involving electronic communications, concerns a claimant who sued an electronic gossip column under state libel law. *See* Steven B. Winters, *The New Privacy Interest: Electronic Mail in the Workplace*, 8 HIGH TECH. L.J. 197, 233 & n.148 (1993) [hereinafter Winters (1993)].

a question of law as to whether their expectations were objectively reasonable.[222]

Given the lack of case law applying tort principles to E-mail interception, predicting future judicial holdings depends on analyzing judicial discussions of similar workplace privacy invasions. A federal district court in *Barksdale v. IBM Corp.*[223] addressed invasion of privacy claims brought by temporary employees stemming from the employer's electronic monitoring of their work performance. In *Barksdale*, the employees were unaware that the employer was monitoring their performance, and they alleged that the employer had invaded their privacy "by eliciting responses from them through its study that it otherwise would not have been able to obtain."[224] In succinctly dismissing their claim, the court stated that "[t]he Defendant's observation and recording of the number of errors the Plaintiffs made in the tasks they were instructed to perform can hardly be considered an intrusion upon the Plaintiffs' 'solitude or seclusion' . . . or [their] private affairs."[225] *Barksdale* thus strongly suggests that E-mail monitoring may not constitute an invasion of privacy, at least where the employer only intercepts work-related communications.

In contrast to *Barksdale*'s curt dismissal regarding electronic monitoring, courts have long recognized a tortious invasion of privacy in situations involving telephone wiretapping,[226] oral communications recording,[227] and personal mail interception.[228] In fact, as a general rule, electronic eavesdropping on the communications of others constitutes an actionable intrusion upon seclusion.[229] Commentators have thus argued that the similarities between E-mail interception and wiretapping, eavesdropping on an individual's conversations, and invasion into one's

---

222. Traynor, *supra* note 127, at S3. The court also held that the interception did not violate state statutes prohibiting wiretapping, eavesdropping, or the recording of confidential communications. *Id.*

223. 620 F. Supp. 1380 (W.D.N.C. 1985), *aff'd*, 1 I.E.R. Cas. (BNA) 560 (4th Cir. 1986).

224. *Id.* at 1382-83.

225. *Id.* at 1383.

226. *See, e.g.*, Nader v. General Motors Corp., 255 N.E.2d 765 (N.Y. 1970); Billings v. Atkinson, 489 S.W.2d 858 (Tex. 1973).

227. Sistok v. Northwest Tel. Sys., Inc., 615 P.2d 176, 182 (Mont. 1980).

228. Vernars v. Young, 539 F.2d 966, 969 (3d Cir. 1976) (holding that plaintiff stated a cause of action in alleging his personal mail had been opened and read by a fellow corporate officer).

229. *See, e.g.*, *Sistok*, 615 P.2d at 182 (holding that surreptitiously recording the conversations of others constituted a cause of action for tortious invasion of privacy); *see also* Griffin, *supra* note 3, at 504-05.

mail support the protection of E-mail under a cause of action for intrusion upon seclusion.[230]

b. Fourth Amendment Cases

Whereas the opinions discussed above provide only limited insight into future E-mail decisions, Supreme Court Fourth Amendment jurisprudence has fundamentally influenced judicial opinions applying all legal sources of privacy protection. The balancing analysis in the tort context is essentially the same in Fourth Amendment jurisprudence, and many state courts have followed the Fourth Amendment balancing approach in addressing tortious invasion of privacy claims.[231] Thus, although the Fourth Amendment does not protect private employees against privacy invasions by their employers,[232] cases from the Fourth Amendment context are critical to discussing how the balancing would apply to private employers' interceptions of employee E-mail.

The landmark case of *O'Connor v. Ortega*[233] is the most recent, most extensive Supreme Court exposition on privacy in the employment context. By grounding employee privacy rights in the "operational realities of the workplace,"[234] *Ortega* has significantly influenced privacy jurisprudence in areas directly relevant to private employees.[235] The

---

230. *See* Witt, *supra* note 181, at 564 (arguing that E-mail should be protected at a level between the complete protection offered written mail under the Federal Mail Statute, 18 U.S.C. § 1702 (1988), and the existing limited protection given E-mail under tort law and the ECPA); *see also* Droke, *supra* note 4, at 178; Baumhart, *supra* note 45, at 925.

231. *See* Baumhart, *supra* note 45, at 938, 947. Although government employees have asserted privacy claims based both on the Fourth Amendment and on a substantive due process right to privacy, courts have only credited the Fourth Amendment claims. *Id.* at 939.

232. The Fourth Amendment does not provide coverage because private employers' actions normally do not constitute state action. *See* Simmons v. Southwestern Bell Tel. Co. 452 F. Supp. 392, 394-95 (W.D. Okla. 1978), *aff'd*, 611 F.2d 342 (10th Cir. 1979). Fourth Amendment rights apply to private sector employees under limited circumstances when the private employer acts under color of federal or state law as a result of the direction of government regulations or law enforcement officials. *See* Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 614-16 (1989) (holding the Fourth Amendment applicable to drug testing conducted by private employers pursuant to government regulations). Constitutional provisions may also apply to private employers that act as government bodies or substantially undertake governmental functions. *See, e.g.*, Marsh v. Alabama, 326 U.S. 501 (1946) (ascribing state actor status to private corporation essentially acting as a municipality in a company-owned town).

233. 480 U.S. 709 (1987). For an extended discussion of *Ortega*, see Winters (1993), *supra* note 220, at 197-202.

234. *Ortega*, 480 U.S. at 717.

235. Winters (1992), *supra* note 11, at 96.

privacy claim in the case stemmed from a state hospital official's search of the office, desk, and file cabinet of a physician suspected of mismanagement of the hospital's residency program.[236] In determining the propriety of the search, the Court held that both the inception and scope of employee searches and surveillance are to be judged according to a case-by-case reasonableness standard "under all [the] circumstances."[237] Under this reasonableness standard, Fourth Amendment rights are violated only if public employees have an expectation of privacy that society is prepared to recognize as reasonable.[238] This privacy expectation "may be reduced by virtue of actual office practices and procedures, or by legitimate regulation."[239] Courts must then balance the employee's reasonable privacy interests against the public employer's need for supervision, control, and efficiency in the workplace.[240] The *Ortega* Court determined that a search conducted by a public employer is reasonable when the employer offers legitimate business reasons for the search such that its needs outweigh the public employee's protected privacy interests.[241]

One problem with the *Ortega* holding is that two of the Court's three criteria for determining the reasonableness of an employee's privacy expectation are not easily applied to advanced technologies such as E-mail, which involve invasions of cyberspace, not physical space.[242] The Court's first criterion looks to what the framers intended the Fourth Amendment to protect. This inquiry is immediately problematic since it is unclear how a court would even go about determining what the framers

---

236. *Ortega*, 480 U.S. at 712-13.

237. *Id.* at 725-26. For a search to be reasonable, the employer must justify it at the inception and must conduct the search so that its scope reasonably relates to the objectives that justified the intrusion. *Id.* at 726; New Jersey v. T.L.O., 469 U.S. 325, 341 (1985). In order for a search to be warranted at its inception, the search must be non-investigatory. If the search is related to an investigation, the employer must have a reasonable suspicion that its search will disclose work-related misconduct. *Ortega*, 480 U.S. at 726.

238. *Ortega*, 480 U.S. at 715.

239. *Id.* at 717.

240. *Id.* at 719-20.

241. *Id.* Thus, the Court's reasoning implies that a workplace search is reasonable under the Fourth Amendment provided the public employer has a legitimate business interest in the search. Witt, *supra* note 181, at 561. The Court held that Ortega had a reasonable expectation of privacy, but because of the procedural posture of the case, the Court did not decide whether the search itself was reasonable. *Ortega*, 480 U.S. at 719, 726-29.

242. Winters (1992), *supra* note 11, at 100. The Court's third criterion inquires into what areas society desires to protect from governmental invasion. *Ortega*, 480 U.S. at 715. The Court applies this criterion in its general balancing analysis. Winters (1993), *supra* note 222, at 197-206.

intended regarding invasions which involve computer technology.[243] The second criterion inquires into how an individual uses a particular space or location. The Court's emphasis on physical space makes its analysis difficult to apply to E-mail communications, where confidentiality can depend upon how one defines space. For instance, if "space" includes an employee's entire E-mail file containing both personal and business communications, a court might conclude that all the messages are non-confidential. In contrast, if an employee has a separate E-mail file for personal communications, a court would presumably consider the file confidential. Furthermore, because E-mail messages are actually stored in the computer network, definitional problems abound in determining whether E-mail files are contained in private offices or public locations.[244]

The *Ortega* decision is also problematic because it adversely affects employee privacy interests by relying on a distorted view of the work-place as one in which employers regularly need to search employee offices and desks for work-related reasons.[245] This view influenced the Court to abandon the warrant and probable cause standard for government-conducted work-related searches as impractical and irreparably damaging to workplace efficiency.[246] By instead utilizing the malleable "reasonableness" standard, the Court evidenced unnecessary deference to employers and provided no concrete protection for employees.[247]

In the application of *Ortega* to cases involving public employees, several federal opinions have interpreted the Court's reasoning in ways that undoubtedly have affected privacy law regarding private employees. Numerous courts have determined that an employee's expectation of privacy can virtually be eliminated by office regulations and practices, and no privacy right is even implicated without such an expectation. For instance, in *Schowengerdt v. General Dynamics Corp.*,[248] the Ninth Circuit embraced the plurality view in *Ortega* by reasoning that specifics in the employment context will determine whether the employee's expectation of privacy is objectively reasonable. In the subsequent appeal to the Ninth Circuit following its remand, the court held that a Navy

243. Winters (1992), *supra* note 11, at 100.

244. *Id.* at 101.

245. *See Ortega*, 480 U.S. at 720-26.

246. Winters (1992), *supra* note 11, at 103-04.

247. *See* Heather L. Hanson, *The Fourth Amendment in the Workplace: Are We Really Being Reasonable?*, 79 VA. L. REV. 243, 246 (1993).

248. 823 F.2d 1328, 1334 (9th Cir. 1987).

civilian engineer's expectation of privacy in his office or desk was not objectively reasonable given the tight security measures, constant searches, and surveillance of employees in his workplace.[249] In *Shields v. Burge*,[250] the Seventh Circuit analyzed the *Ortega* reasonableness standard and established a continuum of work-related justifications that legitimize workplace searches of varying degrees of intrusiveness. These cases, as well as others,[251] suggest that E-mail protection in the private sector will be compromised by employee notification and strong employer interests. Furthermore, *Shields* adds that specific characteristics of the E-mail network that affect the system's confidentiality, such as employees' ability to change their passwords, will affect the level of employer interest needed to justify E-mail interception.[252]

The *Ortega* reasoning was recently applied to the employer's ability to search employee computer files in *Williams v. Philadelphia Housing Authority*.[253] In *Williams* the government employee alleged that his Fourth Amendment rights were violated when his employer removed a computer disk from his desk while he was on leave and read the disk to locate Housing Authority documents. The disk contained work-related material as well as personal items. The federal district court summarily concluded that the employee failed to allege facts sufficient to constitute a claim for unreasonable search and seizure in the workplace, reasoning that *Ortega* gives government employers wide latitude to conduct searches for work-related, non-investigatory purposes. The court further determined that the scope of the search was lawful since the employer reasonably needed to review personal documents in searching for the official documents on the computer disk.[254] *Williams* follows the above cases in suggesting that employers have substantial discretion to conduct searches of employee E-mail. The brevity of the court's opinion is especially troubling in its implication that virtually any legitimate business

---

249. Schowengerdt v. United States, 944 F.2d 483, 488 (9th Cir. 1991), *cert. denied*, 503 U.S. 951 (1992).

250. 874 F.2d 1201, 1208-09 (7th Cir. 1989).

251. *See* American Postal Worker's Union v. United States Postal Serv., 871 F.2d 556, 560 (6th Cir. 1989) (concluding that employee had no reasonable privacy expectation in personal locker given the clear employer inspection policy); Simmons v. Southwestern Bell Tel. Co., 452 F. Supp. 392, 396 (W.D. Okla. 1978) (reasoning, in dicta, that the employee could have no reasonable expectation of privacy under the Fourth Amendment due to the employee's awareness of a company monitoring policy), *aff'd*, 611 F.2d 342 (10th Cir. 1979).

252. *See* Winters (1992), *supra* note 11, at 112.

253. 826 F. Supp. 952 (E.D. Pa. 1993).

254. *Id.* at 954.

interest can justify the interception of personal items that are searched in an effort to locate work-related documents.

In contrast to the above decisions, two cases suggest the limits of the *Ortega* approach. First, a federal district court in *McGregor v. Greer*[255] refused to grant the defendant-employer summary judgment based on an employee's allegations that her employer read "every word" of her private letters while conducting an inventory of her office.[256] Second, a Texas court in *K-Mart Corp. Store No. 7741 v. Trotti*[257] held that a *private* sector employee had a reasonable expectation of privacy in the locker where she stored personal items during work, and which she secured with her own lock, the combination to which she was not required to give to her employer.[258] In finding in her favor, the court stated that "the employee manifested, and the employer recognized, an expectation that the locker and its contents would be free from intrusion and interference."[259] Unlike *Ortega*, *Schowengerdt*, and *Shields*, *Trotti* represents a promising precedent that suggests an employee's expectations of privacy in personal E-mail files is reasonable. However, as with *McGregor*, courts might limit its application to rare instances where the facts are as extreme as in *Trotti*.

Although the case involved a Title III claim concerning the interception of a government employee's oral communications, *Walker v. Darby*[260] raises an important distinction between Fourth Amendment analysis and analysis regarding private employee E-mail privacy. The Eleventh Circuit in *Walker* emphasized the important distinction between traditional Fourth Amendment privacy expectations regarding physical spaces and those regarding the interception and recordation of communications:

---

255. 748 F. Supp. 881 (D.D.C. 1990).

256. *Id.* at 883, 889. The extreme nature of this case is exemplified by the fact that the employer could offer no work-related reason for the search, having already decided to terminate the employee before commencing the search. Hanson, *supra* note 248, at 255.

257. 677 S.W.2d 632 (Tex. Ct. App. 1984), *writ denied*, 686 S.W.2d 593 (Tex. 1985).

258. *Id.* at 638.

259. *Id.* at 637. *But see* Faulker v. Maryland, 564 A.2d 785 (Md. 1989) (finding private employee did not have a reasonable expectation of privacy in a workplace locker, because, in part, company rules clearly established the employer's right to search the lockers when it reasonably suspected drugs to be stored in them).

260. 911 F.2d 1573 (11th Cir. 1990). See *supra* part II for a discussion of Title III as it applies to E-mail interception.

> [The] courts distinguish between an expectation of privacy and the expectation of noninterception that is discussed in §2510(2) [of Title III]. We agree that there is a difference between a public employee having a reasonable expectation of privacy in personal conversations taking place in the workplace and having a reasonable expectation that those conversations will not be intercepted by a device which allows them to be overheard inside an office in another area of a building.[261]

Walker thus suggests that the critical inquiry in E-mail protection should neither be whether the employee has a reasonable privacy expectation that the employer will not invade the physical space where the employee composes, sends, and receives E-mail messages nor whether the employer will otherwise indirectly come upon the contents of E-mail communications. Rather, the issue should be whether the employee has an expectation that the employer will not override employee password protection and directly monitor and record E-mail messages from the network. In this vein, the *Walker* court stated: "[W]hile Walker might have expected conversations uttered in a normal tone of voice to be overheard by those standing nearby, it is highly unlikely that he would have expected his conversations to be electronically intercepted and monitored in an office in another part of the building."[262]

Taken collectively, the above cases have interpreted government employees' privacy interests under the Fourth Amendment so narrowly that one commentator has stated that these rights "have all but vanished completely."[263] The reasonable expectation analysis appears to be entirely within the employer's control, and the reasonableness standard limiting the scope of the intrusion is unnecessarily deferential to employers and provides employees with no absolute protection.[264] In sum, employee monitoring limited to work-related activities or communications almost certainly will not implicate Fourth Amendment protection, either because the employee is notified of the monitoring or because the monitoring is deemed relatively unintrusive by the courts.[265]

---

261. *Walker*, 911 F.2d at 1579 (footnote omitted).

262. *Id.*

263. Winters (1992), *supra* note 11, at 116 (citing Erwin Chemerinsky, *The Supreme Court Foreword: The Vanishing Constitution*, 103 HARV. L. REV. 43, 96-98 (1989)).

264. Hanson, *supra* note 248, at 246.

265. Jenero & Mapes-Riordan, *supra* note 5, at 79.

Fourth Amendment law remains unclear only as to whether an employer may lawfully conduct searches of personal information for reasons not related to business or criminal activities.[266] By emphasizing the personal content of the information searched, cases such as *McGregor* implicitly recognize an emerging constitutional protection of informational privacy and imply that the personal content of the accessed information is relevant to finding a Fourth Amendment violation, and in turn, a violation under tort law.[267] Furthermore, because the employee's privacy expectation is heightened regarding personal information, the employer may have to demonstrate an individualized suspicion of misconduct to justify such a search.[268] The above cases also distinguish between a search or interception for a legitimate business purpose and one that overrides its bounds, especially if the employee is not notified of the search.[269] At the same time, these cases address the importance of balancing the interests between public employers and their employees by applying more lenient standards to searches when the government's interest is most compelling.[270]

c. Application to E-mail Monitoring

From this analysis, E-mail monitoring and communication interception will more likely be tortious if the monitoring is aimed at the employee's personal or private affairs than if the monitoring is confined to work-related activities.[271] Employer intrusions that explicitly overreach to

266. For example, although an employer may have a legitimate interest in searching an employee's desk for work-related purposes, it is uncertain whether the employer can read personal information in the desk after it obtains the needed business information. Witt, *supra* note 181, at 561 (citing O'Connor v. Ortega, 480 U.S. 709, 723 (1987)).

267. *See generally* Whalen v. Roe, 429 U.S. 589, 599-600 (1977); Doe v. Borough of Barrington, 729 F. Supp. 376, 382 (D.N.J. 1990) (both recognizing that the Constitution protects one's privacy rights against the disclosure of personal information); Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy*, 10 N. ILL. U. L. REV. 479, 481, 492-93 (1990) (arguing that tort and constitutional law provide a right to informational privacy).

268. Jenero & Mapes-Riordan, *supra* note 5, at 79.

269. Witt, *supra* note 181, at 561.

270. *See, e.g.*, Skinner v. Railway Labor Executives' Ass'n., 489 U.S. 602, 626-27 (1989) (protecting public safety); Harmon v. Thornburgh, 878 F.2d 484, 492 (D.C. Cir. 1989) (protecting sensitive information), *cert. denied*, 493 U.S. 1056 (1990); Shields v. Burge, 874 F.2d 1201, 1204 (7th Cir. 1989) (eliminating police misconduct).

271. *See, e.g.*, Pemberton v. Bethlehem Steel Corp., 502 A.2d 1101, 1117 (Md. Ct. Spec. App. 1986) (holding that evidence showing that employer had probably placed a detection device above the door of the employee's motel room and conducted surveillance was sufficient to prevent summary judgment in favor of the employer on the employee's

intercept personal E-mail messages are not justified by the employer's basic need for an efficient workplace.[272] In fact, an employer seemingly would only be justified in deliberately intercepting personal messages if it reasonably suspected that such communications would reveal involvement in activity seriously inimical to the employer's interests. Thus, an employer will likely exceed its authority if it examines E-mail files clearly marked personal in an attempt to locate certain work-related files, especially if no employer policy addresses whether employees may send personal messages through the workplace E-mail network. Under these circumstances, the rationale for conducting the search no longer reasonably relates to the actual scope of the search, and the employer commits an unreasonable intrusion.[273]

Employer monitoring of E-mail communications might also be limited because many of the employer's rationales for monitoring telephone calls or surveying the workplace do not exist in the E-mail context. For instance, employers often monitor employee telephone calls when the employees use the telephone to perform primary work functions such as telemarketing and customer service.[274] Employers in these industries need to utilize such monitoring because their "product is the phone calls" and because monitoring is the only way employers can survey their employees' work product.[275] In contrast, employees rarely use E-mail to converse with customers. Instead, E-mail service is largely used as an electronic alternative to intra-office written memoranda or phone lines.[276] Given this distinction, an employer's interception of E-mail does not directly ensure the quality of the product or service the employer offers to its clients or customers. Indeed, employer interception normally only

---

privacy claim), *cert. denied*, 508 A.2d 488 (Md. 1986), *cert. denied*, 479 U.S. 984 (1986); KEETON ET AL., *supra* note 188, § 117, at 855-56 (discussing when a potential plaintiff's actions are private enough to give rise to an action for intrusion).

272. Plaintiffs in an E-mail law suit, however, may experience difficulty in attempting to prove that activities allegedly intruded upon were, in fact, private and personal.

273. *See* Witt, *supra* note 181, at 562.

274. Jenero & Mapes-Riordan, *supra* note 5, at 72; *see* Shoop, *supra* note 6, at 13 (stating that telecommunications and customer service employees are most likely to be monitored electronically although any employee who uses a computer or telephone is a candidate for such monitoring); Ann K. Bradley, *An Employer's Perspective on Monitoring Telemarketing Calls: Invasion of Privacy or Legitimate Business Practice?*, 42 LAB. L.J. 259, 259 (1991) (concluding that supervisors can randomly monitor the performance of workers whose primary responsibilities involve using the telephone).

275. Shoop, *supra* note 6, at 14 (statement of Mac Hansbrough, operator of a telemarketing business in Washington, D.C.).

276. *But cf.* Klemens, *supra* note 28 (arguing that E-mail systems benefit employers if the employers directly connect their networks to those of their clients).

serves the less cogent goal of minimizing frivolity on the job, and the efforts at such interception would arguably be spent more effectively in monitoring the actual work product of the employees.

These arguments advocating limited interceptions nevertheless remain ineffectual given the current common law deference to the employer's business rationales. Regardless of whether monitoring personal communications actually increases productivity, employer actions seem justified as long as their interests in the intrusion are work-related.[277] Ultimately, the tort analysis remains a balancing act and private employees can never be certain of any absolute privacy protections; their privacy extends only to the point where an employer can offer no legitimate business justification for the intrusion.

Moreover, even if an employer's interests are illegitimate, common law protection is inadequate because employers may alter employee privacy expectations by modifying workplace procedures, such as by publicizing monitoring policies[278] or by requiring employees to submit to invasive background checks.[279] Furthermore, the employer that owns and operates the E-mail network can present especially strong arguments why employees should not expect their messages to be private,[280] and without a subjective privacy expectation, the court does not analyze the proffered business justifications because no legally cognizable privacy interest is implicated.[281] The employer's best defense to common law liability is thus to publish a detailed E-mail monitoring policy that warns employees that messages may be monitored despite system features that create a sense of privacy.[282] Indeed, both the employer's qualified privilege of protecting legitimate business interests and the legal privilege of consent

---

277. *See* Jenero & Mapes-Riordan, *supra* note 5, at 83 (noting that employers' actions remain justified even if they use highly intrusive electronic monitoring techniques).

278. *See* Schowengerdt v. United States, 944 F.2d 483, 488-89 (9th Cir. 1991), *cert. denied*, 503 U.S. 951 (1992); American Postal Workers Union v. United States Postal Serv., 871 F.2d 556, 560 (6th Cir. 1989).

279. National Fed'n of Fed. Employees v. Cheney, 884 F.2d 603, 612-13 (D.C. Cir. 1989), *cert. denied*, 493 U.S. 1056 (1990).

280. *See* Heredia, *supra* note 3, at 331-32. *See generally* Linowes & Spencer, *supra* note 2, at 593 (stating that employers are normally given the right to monitor the workplace because they own the telephone system and the workplace premises and because they control other factors affecting the monitoring).

281. *See generally* Griffin, *supra* note 3, at 505; KEETON ET AL., *supra* note 188, § 117, at 867-68 (establishing consent as a defense).

282. Baumhart, *supra* note 45, at 941; *see also* McCloskey v. Honolulu Police Dep't, 799 P.2d 953, 959 (Haw. 1990); *cf.* Bratt v. IBM Corp., 785 F.2d 352, 360-61 (1st Cir. 1986) (noting that the presence of employer privacy regulations may serve to enhance an already existing privacy expectation).

serve as formidable obstacles to an employee's invasion of privacy cause of action.

B. State Constitutional Law

1. Constitutional Privacy Rights

Many states have constitutional provisions that parallel the Fourth Amendment's proscriptions against unreasonable searches and seizures.[283] Unlike the federal constitution, however, at least ten state constitutions explicitly grant their citizenry a right to privacy.[284] Six of these states provide only a general right to privacy.[285] Three other states, Florida, Illinois, and Louisiana, specifically protect the privacy of communications,[286] while South Carolina protects against unreasonable searches, seizures, and invasions of privacy.[287] State courts have applied these privacy protections more expansively than Fourth Amendment protections;[288] to date, however, only California has expressly determined that its constitutional right of privacy embodies a cause of action against nongovernmental entities such as private employers.[289] This distinction,

---

283. Jenero & Mapes-Riordan, *supra* note 5, at 80.

284. Griffin, *supra* note 3, at 510 n.123.

285. *See* ALASKA CONST. art. I, § 22; ARIZ. CONST. art. II, § 8; CAL. CONST. art. I, § 1; HAW. CONST. art. I, § 6; MONT. CONST. art. II, § 10; WASH. CONST. art. I, § 7.

286. *See* FLA. CONST. art. I, § 12 ("The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, and against the unreasonable interception of private communications by any means, shall not be violated."); ILL. CONST. art. I, § 6 ("The people shall have the right to be secure in their persons, houses, papers, and other possessions against unreasonable searches, seizures, invasions of privacy, or interceptions of communications by eavesdropping devices or other means."); LA. CONST. art. I, § 5 ("Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy."). Florida's constitution also provides a general right to privacy. FLA. CONST. art. I, § 23.

287. *See* S.C. CONST. art. I, § 10 ("The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and unreasonable invasions of privacy shall not be violated.").

288. Heredia, *supra* note 3, at 313.

289. *E.g.*, Hill v. National Collegiate Athletic Ass'n, 865 P.2d 633, 641 (Cal. 1994); Luck v. Southern Pac. Trans. Co., 267 Cal. Rptr. 618, 627-29 (Ct. App.), *cert. denied*, 498 U.S. 939 (1990); Semore v. Pool, 266 Cal. Rptr. 280, 283-84 (Ct. App.), *review denied*, 217 Cal. App. 3d 1087 (Cal. 1990); Wilkinson v. Times Mirror Corp., 264 Cal. Rptr. 194, 198-200 (Ct. App. 1989). In addition to the California cases, the Louisiana case of Saint Julien v. South Central Bell Tel. Co., 433 So. 2d 847, 851 (La. Ct. App. 1983), determined that article one, section five of the Louisiana Constitution may apply to a telephone company's unauthorized entry into a subscriber's apartment to repossess telephones. Commentators have suggested that this holding implies that Louisiana may also

coupled with the fact that California privacy law is well developed in the private employment context, suggests that California can serve as a model to identify potential state concerns.[290]

California courts will likely determine that employer E-mail monitoring violates the state constitution in some circumstances.[291] Courts could readily infer such a cause of action since California courts have already held the state constitution to cover the collection of information by private businesses.[292] Furthermore, the ballot pamphlet argument in support of the passage of the state constitutional privacy provision interpreted the provision as granting a right to be left alone and a right to be free from the collection of personal information.[293] The first issue in confronting an E-mail claim would surround whether the intercepted information was "private." Employers would undoubtedly assert that employee information transmitted over employer E-mail networks is necessarily not private and thus not deserving of protection. A California appellate court in *Soroka v. Dayton Hudson Corp.*,[294] however, extended the constitutional provision to protect the gathering of "unnecessary information" about job applicants. From this broad interpretation, courts could certainly reason that the interception of the content of many E-mail messages is unnecessary to the employer's interest in ensuring workplace efficiency.[295]

Given the potential protection afforded to employee E-mail communications in California, the critical issue is the standard employers need to satisfy in order to avoid infringing the state constitutional right to privacy. Before the 1994 California Supreme Court case of *Hill v. National Collegiate Athletic Ass'n*,[296] California appellate courts appeared to agree that private employers must demonstrate a compelling interest in order to invade employee privacy.[297] *Hill*, however, extensively analyzed the

---

extend constitutional privacy protections to private employees. *See* Griffin, *supra* note 3, at 511.

290. *See* Traynor, *supra* note 127, at S3; Victoria Slind-Flor, *What Is E-Mail, Exactly?*, NAT'L L.J., Nov. 25, 1991, at 22 (quoting Robert Ellis Smith, editor of the *Privacy Journal*, as stating that California court decisions "will probably be a model for the nation").

291. Heredia, *supra* note 3, at 332.

292. *See* Valley Bank v. Superior Court, 542 P.2d 977, 979 (Cal. 1975).

293. Heredia, *supra* note 3, at 332.

294. 1 Cal. Rptr. 2d 77, 86 (Ct. App. 1991), *review granted*, 822 P.2d 1327 (Cal. 1992), *review dismissed*, 862 P.2d 148 (Cal. 1993).

295. *See* Heredia, *supra* note 3, at 333.

296. 865 P.2d 633 (Cal. 1994).

297. *See Soroka*, 1 Cal. Rptr. 2d at 86 (Ct. App. 1991) (applying compelling interest standard to job applicant privacy claim); Luck v. Southern Pac. Transp. Co., 267 Cal. Rptr. 618, 631-32 (Ct. App.) (applying compelling interest standard to employee privacy claim),

legislative history of the state constitutional provision, the common law right to privacy, and the right to privacy embodied in the U.S. Constitution, concluding that the NCAA need not demonstrate a compelling interest in order to conduct random drug testing of athletes.[298] In reaching its conclusion, the court drew a distinction between invasions of interests "fundamental to personal autonomy,"[299] which require a compelling interest, and invasions of "less central" privacy interests, which require only countervailing interests.[300] From this distinction, the court generally established a test under which the privacy interests at issue must "be specifically identified and carefully compared with *competing* or *countervailing* privacy and nonprivacy interests in a 'balancing test.'"[301] The court further reasoned that a plaintiff may rebut a defendant's proffered justifications for the intrusion by demonstrating that the defendant could have utilized effective alternatives that have a lesser impact on privacy interests.[302] Applying these standards to the facts in the case, the court concluded that the NCAA's drug testing program impacted legally protected privacy interests but that its program did not violate the California Constitution because the athletes' privacy interests were reduced by their voluntary participation in intercollegiate athletics.[303]

Given the *Hill* court's distinction between autonomy privacy and other "less central" privacy interests, the decision undoubtedly suggests that

---

cert. denied, 498 U.S. 939 (1990); Heredia, *supra* note 3, at 326-29. *But see* Wilkinson v. Times Mirror Corp., 264 Cal. Rptr. 194, 198-200 (Ct. App. 1989) (holding that private employer need not demonstrate a compelling interest to require job applicants to undergo drug testing, as long as the privacy right was not substantially burdened or affected). *See generally* Porten v. University of San Francisco, 134 Cal. Rptr. 839, 843 (Ct. App. 1976) (applying the compelling interest standard to the release of personal information by a private university).

298. *Hill*, 865 P.2d at 654.

299. Such interests include the "freedom from involuntary sterilization or the freedom to pursue consensual familial relationships." *Id.* at 653.

300. *Id.* (reasoning that "[t]he particular context, i.e., the specific kind of privacy interest involved and the nature and seriousness of the invasion and any countervailing interests, remains the critical factor in the analysis").

301. *Id.* at 655 (emphasis added). In deciding that the NCAA's interest need not be compelling, the court emphasized that the NCAA was a private actor, less likely to pose a significant threat to privacy interests than governmental bodies. *Id.* at 656. Dissenting Justices George and Mosk, each writing separate opinions, would have required the NCAA to offer a compelling interest. *Id.* at 672 (George, J., dissenting); *id.* at 682-83 (Mosk, J., dissenting).

302. *Id.* at 657.

303. *Id.* at 657-69. The court added that its holding implied no views about employer drug testing because employment settings are "diverse, complex, and very different from intercollegiate athletic competition." *Id.* at 667.

private employers need not demonstrate a compelling interest in order to invade employee E-mail.[304] Instead, a private employer may prevail against a state constitutional privacy claim if it proves as an affirmative defense that the invasion substantively furthered a "competing," "legitimate" countervailing interest.[305] In balancing the employer's interests and the employee's privacy expectations, the *Hill* court's analysis implies that courts will not give the privacy interests significant weight.[306] Thus, as in the common law and Fourth Amendment contexts, employers' proffered interests will probably outweigh employee privacy interests in California's constitutional balancing.

Private employee privacy interests are most likely to be protected under the *Hill* analysis if the employee demonstrates that the employer can serve its business interests through less intrusive means. For instance, if the employer offers general justifications for E-mail monitoring such as improving workplace quality control, employees could easily suggest less intrusive alternatives by which the employer could achieve its objective, such as more frequent reviews of employee work product. Because *Hill* reasons that the alternatives must be supported by substantial evidence on appeal,[307] the employee-plaintiffs must be able to offer studies or expert opinions supporting the ability of alternative measures to monitor workplace efficiency sufficiently. Ultimately, however, this opportunity to vindicate employee privacy appears speculative at best, especially if the employer can proffer business interests that can only be satisfied through E-mail monitoring.

2. *State Public Policy*

Although *Hill* effectively limits the ability of private employees in California to maintain a cause of action directly based on the state constitutional privacy right, employees might prevail by asserting that the

---

304. *See id.* at 668 (reasoning that the court in Luck v. Southern Pac. Trans. Co., 267 Cal. Rptr. 618, 629 (Ct. App.), *cert. denied*, 498 U.S. 939 (1990), "erroneously" applied the compelling interest test in the drug testing context).

305. *See id.* at 655-57.

306. *Id.* at 648 (citing Kelso, *supra* note 218, at 376). Given the application of this balancing, an employee litigating an E-mail claim cannot rely on California appellate decisions that applied the compelling interest standard to drug testing by private employers, especially if courts view E-mail interception as less invasive than drug testing. *Cf. Luck*, 267 Cal. Rptr. at 632; Semore v. Pool, 266 Cal. Rptr. 280, 283 (Ct. App.), *review denied*, 217 Cal. App. 3d 1087 (Cal. 1990).

307. *See Hill*, 865 P.2d at 664.

constitutional provision supports a state public policy favoring regulation of intrusions in the private workplace.[308] Finding a state public policy would allow an employee to proceed on some form of constitutional tort theory,[309] even if the employer has only attempted to invade the employee's personal privacy.[310] *Semore v. Pool*[311] and *Luck v. Southern Pacific Transportation Co.*[312] are two California appellate court decisions that addressed such causes of action when employees were terminated for refusal to submit to employer drug testing.[313] Although these pre-*Hill* courts agreed that the employers must establish a compelling interest to justify the intrusion,[314] the courts disagreed as to whether the resulting termination gave rise to a cause of action for wrongful termination in violation of public policy.[315] In recognizing the cause of action, the court in *Semore* reasoned that the privacy right "is unquestionably a fundamental interest of our society."[316] In contrast, the court in *Luck* determined that the employee had stated no cause of action by reasoning that "the right to privacy is, by its very name, a private right and not a public one."[317] Thus, assuming that the countervailing balancing standard in *Hill* will apply to private employer invasions of employee E-mail, employees in California will face two hurdles in maintaining a successful public policy cause of action for E-mail interception: first, they must counter any employer interest that the employer proves legitimate; and second, they must convince the court that the right to privacy benefits the public at large as well as the particular employees in the action.[318]

In the other states that have not explicitly held their constitutional provisions applicable to private employers, a cause of action based on a public policy violation is an employee's only recourse to relate the

---

308. Baumhart, *supra* note 45, at 938; *see also* Heredia, *supra* note 3, at 329 (arguing that the state constitution itself may provide the duty element in a tort cause of action). *But cf.* Barnett & Makar, *supra* note 17, at 747 (reasoning that Florida's decision not to extend its constitutional protections to intrusions by private parties evidences an intent that such intrusions are not to be elevated to the constitutional level).

309. Baumhart, *supra* note 45, at 943.

310. *See* Heredia, *supra* note 3, at 321-24.

311. 266 Cal. Rptr. 280 (Ct. App.), *review denied*, 217 Cal. App. 3d 1087 (Cal. 1990).

312. 267 Cal. Rptr. 618, 629 (Ct. App.), *cert. denied*, 498 U.S. 939 (1990).

313. Heredia, *supra* note 3, at 321-24.

314. *Semore*, 266 Cal. Rptr. at 283; *Luck*, 267 Cal. Rptr. at 632.

315. Heredia, *supra* note 3, at 321-24.

316. *Semore*, 266 Cal. Rptr. at 285.

317. *Luck*, 267 Cal. Rptr. at 635.

318. *See* Heredia, *supra* note 3, at 321-24.

constitutional provisions to private employers.[319] As in California, these employees may bring a wrongful discharge action based on the employer's breach of the implied covenant of good faith and fair dealing.[320] To this end, the Alaska Supreme Court in *Luedtke v. Nabors Alaska Drilling, Inc.*[321] held that its state constitutional right to privacy embodied a public policy disfavoring certain private employer privacy intrusions. However, several state court opinions, such as *Barr v. Kelso-Burnett Co.*,[322] have expressly rejected the grounding of a state public policy relevant to private employers in a state constitutional right to privacy.[323] The holding in *Barr* follows the consistent holdings that the U.S. Constitution does not support a public policy that would provide the basis for a wrongful discharge action.[324]

Given the present limitations, state constitutions remain insufficient in their protection of private employees' privacy. The employee who bases a claim on a state constitutional right must overcome too many hurdles to establish employer liability. Even if the state allows a private employee to pursue a specific privacy claim against a private employer—a claim that is currently only possible in California—the employee must confront the same balancing analysis as in the tort context, an analysis that favors employers that proffer legitimate business justifications for their E-mail monitoring. Moreover, existing state constitutions do not provide the needed comprehensive protection because few private employees in America can bring a cause of action directly under their respective state constitution.

---

319. Baumhart, *supra* note 45, at 938.

320. Numerous states have recognized a claim for wrongful discharge. Droke, *supra* note 4, at 179 (citing Payne v. Rozendaal, 520 A.2d 586 (Vt. 1986); Harles v. First Nat'l Bank, 246 S.E.2d 270 (W. Va. 1978)).

321. 768 P.2d 1123, 1131-32 (Alaska 1989). *Accord* Cordle v. General Hugh Mercer Corp., 325 S.E.2d 111, 117 (W. Va. 1984) (holding that state public policy was violated when an employee was terminated for refusing to submit to a random polygraph test as a condition of continued employment).

322. 478 N.E.2d 1354, 1356-57 (Ill. 1985).

323. *See* Hennessey v. Coastal Eagle Point Oil Co., 609 A.2d 11 (N.J. 1992) (holding that employer's discharge of employee in safety sensitive position for refusing to submit to drug testing did not violate a clear mandate of public policy under state constitution); Booth v. McDonnell Douglas Truck Serv., Inc., 585 A.2d 24 (Pa. Super. Ct. 1991) (rejecting the argument that the Pennsylvania Constitution provides the public policy needed to maintain a wrongful discharge action); Hershberger v. Jersey Shore Steel Co., 575 A.2d 944 (Pa. Super. Ct. 1990) (same).

324. *E.g.*, Johnson v. Carpenter Technology Corp., 723 F. Supp. 180, 185-86 (D. Conn. 1989); Borse v. Piece Goods Shop, 758 F. Supp. 263, 268 (E.D. Pa. 1991).

C. *State Statutory Law*

Regardless of the unavailability of state constitutional relief, all but four states have statutes restricting the interception of wire communications.[325] In passing these laws, state legislators have generally sought to balance employees' privacy interests with employers' interests in assessing employee performance.[326] Courts have traditionally interpreted Title III and the ECPA as preempting state legislation only where the state law is less protective of individual freedoms than federal law.[327]

Many of these state wiretapping statutes parallel Title III coverage by providing exemptions to liability, including business-extension exceptions and exceptions when one party to the communication consents to the interception.[328] Akin to tort protection of privacy interests, a primary element in each wiretapping statute is whether the claimant had a reasonable expectation of privacy in the communication.[329] Some state wiretapping laws, however, may not provide adequate restitution to affected employees because the laws' primary remedy is penal, precluding a civil cause of action by an employee to obtain damages.[330]

Some states offer greater protection than the ECPA,[331] often by requiring that all parties to the communication consent to the interception in order for it to be lawful.[332] Some states also provide more protection

---

325. *See* ROBERT ELLIS SMITH, COMPILATION OF STATE & FEDERAL PRIVACY LAWS 60-63 (1992). The District of Columbia also has a wiretap statute. *Id.* at 60. The four states that do not have wiretapping statutes are Mississippi, Missouri, South Carolina, and Vermont. *Id.* at 60-63. Of these four, South Carolina appears to be the only state that has not provided comparable protection in other electronic surveillance or monitoring statutes. *See* Jenero & Mapes-Riordan, *supra* note 5, at 94.

326. Griffin, *supra* note 3, at 519.

327. *See, e.g.*, United States v. McKinnon, 721 F.2d 19, 21 n.1 (1st Cir. 1983); Evans v. State, 314 S.E.2d 421, 425 (Ga.), *cert. denied*, 469 U.S. 826 (1984); *see also Hearings on S. 1667*, *supra* note 115, at 105-06 (statement of P. Michael Nugent, Board Member, ADAPSO) (arguing that the ECPA needed express preemption clause in order to prohibit more stringent state laws); S. REP. NO. 1097, 90th Cong., 1st Sess. (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2181 (evidencing congressional intent that states be allowed to promulgate stricter state wiretapping laws).

328. *See* Griffin, *supra* note 3, at 519-20; Fitzpatrick (1992), *supra* note 3, at 1174 (stating that thirty states have statutes that mirror Title III protections).

329. Droke, *supra* note 4, at 174.

330. *Id.* at 173 (citing SMITH, *supra* note 326, at 38-39).

331. *See, e.g.*, MD. CODE ANN., CTS. AND JUD. PROC. §§ 10-402(a)(3), 10-401(4)(I) (1989 and Supp. 1994); *see also* Barnett & Makar, *supra* note 17, at 744 n.159 (providing statutory citations for state wiretapping laws); Baumhart, *supra* note 45, at 945; SMITH, *supra* note 326, at 60-63 (providing citations and key passages of state wiretapping laws).

332. Statutes in California, Delaware, Florida, Illinois, Louisiana, Maryland, Massachusetts, Michigan, Montana, Oregon, Pennsylvania, and Washington require the

because they do not include consent exceptions or business-extension or business use exceptions.[333] Additionally, other states exempt only communications "common carriers" under their provider exceptions, as opposed to the ECPA, which more generally exempts providers of "electronic communications services."[334] This limitation to "common carriers" could create liability for employer-providers who would be exempted under the ECPA. Furthermore, Pennsylvania prohibits the interception of even transactional information regarding telecommunications.[335]

This broader protection under some state laws is supplemented when state courts construe state provider or business-extension exceptions more narrowly than federal courts' construction of the exceptions in Title III and the ECPA. For instance, the California Supreme Court has held that the exception in its wiretapping statute exempting the use of any instrument "furnished and used pursuant to the tariffs" of a communications provider does not exempt the use of extension telephones for eavesdropping on confidential communications.[336] Additionally, an intermediate Florida appellate court has held that the state provisions authorizing interceptions of communications are statutory exceptions to the federal and state constitutional right to privacy and as such should be narrowly construed.[337] At the same time, however, courts have interpreted state statutes in ways that defy their express terms.[338] For instance, although the statutes explicitly require all-party consent, courts have interpreted the Delaware and Illinois statutes to require the consent

---

consent of all parties to the communication. Jenero & Mapes-Riordan, *supra* note 5, at 94 n.36; *see* SMITH, *supra* note 326, at 60-63. To increase protection, Florida's statute also creates a civil cause of action allowing the recovery of actual and punitive damages as well as attorneys' fees. FLA. STAT. Ch. 934.10 (1994).

Because of these differences in the state statutes, employer interceptions involving interstate E-mail communications may be legal in the sending state but not in the receiving state. The location of the interception normally determines which state law governs, but determining the location may be circular because that determination, in turn, depends on the definition of interception in the governing statute. *See* Kirk W. Munroe, *Commercial Eavesdropping: A Catch 22*, 63 FLA. B.J., Mar. 1989, at 12 n.10.

333. *See* Lee, *supra* note 25, at 175 (Table 2) (listing state statutes that provide consent and business use exceptions).

334. *Id.* at 152.

335. *See* 18 PA. CONS. STAT. ANN. § 5771 (Supp. 1994).

336. Ribas v. Clark, 696 P.2d 637, 642 (Cal. 1985).

337. *See* Barnett & Makar, *supra* note 17, at 748 (citing Copeland v. State, 435 So. 2d 842 (Fla. Dist. Ct. App.), *review denied*, 443 So. 2d 980 (Fla. 1983)).

338. Jenero & Mapes-Riordan, *supra* note 5, at 95.

of only one of the parties to the communication in order for the interception to be lawful.[339]

Unlike the ECPA, many state wiretapping laws do not specifically cover electronic communications.[340] In such instances, employees might argue that courts should interpret the laws to include protection for workplace E-mail communications. Employees might first argue that state wiretapping laws reflect general legislative intent to protect the privacy and confidentiality of all communications, such as E-mail, that travel across telephone lines.[341] Furthermore, because E-mail messages are transmitted via keyboards, they may be analogized to telegraphic communications, which are specifically covered in many state statutes.[342]

As an example, California employees might attempt to argue that state statutes prohibiting wiretapping[343] and eavesdropping[344] protect workplace E-mail privacy. Although the eavesdropping statute may be more applicable to E-mail than the wiretapping statute because the law is not restricted to wire-based communication,[345] the eavesdropping statute, unlike the wiretapping statute, provides a critical exception when the parties to the communication reasonably expect to be overheard or recorded.[346] More importantly, a California appellate court has held that the wiretapping statute applies to interceptions by an unauthorized connection to the transmission line whereas the eavesdropping statute applies when the interception equipment is not connected to the transmission line.[347] Most employer E-mail interceptions would thus be governed by the wiretapping statute. If either California statute applies, their

---

339. *Id.* at 94 n.36, 95 n.37 (citing United States v. Vespe, 389 F. Supp. 1359, 1372 (D. Del.), *aff'd*, 520 F.2d 1369 (3d. Cir. 1975), *cert. denied*, 423 U.S. 105 (1976); People v. Beardsley, 503 N.E.2d 346, 350 (Ill. 1986)).

340. *See* SMITH, *supra* note 326, at 60-63.

341. Droke, *supra* note 4, at 182-83.

342. *Id.* at 183. For an example of a state statute covering telegraphic communications, see ARK. CODE § 23-17-107 (Michie 1987). *See generally* SMITH, *supra* note 326, at 60-63 (discussing all state wiretap laws, including some statutes covering telegraphic communications).

343. CAL. PENAL CODE § 631(a) (West 1988 & Supp. 1995).

344. CAL. PENAL CODE § 632 (West Supp. 1995).

345. Droke, *supra* note 4, at 184. Under the statute, eavesdropping is illegal "whether the communication is carried on among such parties [in person] . . . or by means of a telegraph, telephone, or other device." CAL. PENAL CODE § 632(a) (West Supp. 1995).

346. CAL. PENAL CODE § 632(c) (West Supp. 1995). As in the wiretap statute, § 631(b), correctional facilities and public utilities are excepted from liability in the eavesdropping statute, § 632(e).

347. Winters (1993), *supra* note 222, at 197-216 (citing People v. Ratekin, 261 Cal. Rptr. 143 (Ct. App. 1989)).

liability exceptions are narrower than the ECPA because they allow interception only if *both* parties consent.[348] They also provide a civil cause of action with recovery of $5,000 or three times the plaintiff's actual damages.[349]

An important case testing the applicability of California statutes to E-mail privacy has been *Flanagan v. Epson America, Inc.*[350] *Flanagan*, and its companion case *Shoars v. Epson America, Inc.*,[351] are two of the first cases in the nation to address E-mail privacy rights in the private sector workplace.[352] Both cases concern an employee, Alana Shoars, who worked as an office systems programmer and analyst and was responsible for providing employees with training and support in using the office E-mail system. Shoars believed that no one had authority to intercept and read the E-mail transmissions and informed the employees that their messages would remain confidential. Upon discovering that her supervisor had been intercepting and reading all E-mail messages entering and leaving the office via MCI mail, Shoars demanded that he stop intercepting the communications. After she subsequently sought an E-mail account number to which her supervisor would not have access, her supervisor fired her for gross insubordination.[353] In *Shoars*, Shoars sued Epson under California Penal Code section 631, which provides a private cause of action for illegal interception of private wire communications.[354] In *Flanagan*, about 700 Epson employees who use E-mail through their desktop computers brought a class action suit against the company under section 631.[355]

In *Shoars*, the superior court summarily rejected Shoars' claim that Epson's actions constituted a violation of California's wiretapping law. The court reasoned that the legislative history behind the wiretapping statute evidences concern about the "danger of technology" in general and

---

348. CAL. PENAL CODE §§ 631(a), 632(a) (West 1988 & Supp. 1995).

349. CAL. PENAL CODE § 637.2 (West 1988 & Supp. 1995).

350. Flanagan v. Epson Am., Inc., No. BC007036 (Cal. Super. Ct. Jan. 4, 1991).

351. No. B073243 (Cal. Ct. App.), *review denied*, No. S040065, 1994 Cal. LEXIS 3670 (Cal. June 29, 1994).

352. Caldwell, *supra* note 22, at 34. For additional information on the *Shoars* and *Flanagan* cases, see Don J. DeBenedictis, *E-Mail Snoops*, A.B.A. J., Sept. 1990, at 26, 27.

353. Winters (1992), *supra* note 11, at 120-21; *see also* Griffin, *supra* note 3, at 493 n.3 (summarizing the *Shoars* case as well as other current cases involving E-mail privacy).

354. Winters (1992), *supra* note 11, at 121 (citing CAL. PENAL CODE § 631 (West 1988 & Supp. 1995)).

355. Flanagan v. Epson Am., Inc., No. BC007036, slip op. at 1-2 (Cal. Super. Ct. Jan. 4, 1991). The court rejected the class certification for the case on July 31, 1992. *Electronic Mail Raises Issues About Privacy, Experts Say*, *supra* note 22, at A7.

not specifically about the interception of E-mail transmissions.[356] In *Flanagan*, the superior court presented a written opinion offering two reasons for rejecting the employees' claim. First, the court determined that it was not clear that the employees had an expectation of privacy, which was a required element for an invasion of privacy action. Second, and more importantly, the court reasoned that, even assuming the employees had such an expectation, E-mail was not covered under section 631 in light of the California Supreme Court's interpretation of the statute in *Ribas v. Clark*.[357] The court concluded:

> Although it may well be that plaintiffs' right of privacy with respect to the electronic communications described in the complaint ought to be, as a matter of public policy, entitled to protection, the court believes that such an extension to Penal Code § 631, if it is to be made, is the proper province of the Legislature, which is better equipped than a court to determine the precise nature of such an extension, as well as appropriate exceptions and exemptions therefrom. In this connection, the court notes that the U.S. Congress has enacted separate statutes pertaining to Wire and Electronic Communications Interception and Interception of Oral Communications and pertaining to Stored Wire and Electronic Communications and Transactional Records Access.[358]

The court's reasoning in *Flanagan* is problematic for several reasons. First, the court overlooked the distinction in *Walker v. Darby*[359] and *Ribas v. Clark*[360] between an expectation of privacy and an expectation of noninterception.[361] From the reasoning in these cases, the Epson employees should have retained a cause of action as long as they were unaware of the precise nature of their employer's intrusive actions.[362]

---

356. Griffin, *supra* note 3, at 493 n.3 (citing Telephone Interview with Noel Shipman, Attorney for Alana Shoars (Mar. 12, 1991)).

357. 696 P.2d 637 (Cal. 1985).

358. *Flanagan*, slip op. at 4 (citations omitted).

359. 911 F.2d 1573, 1579 (11th Cir. 1990).

360. 696 P.2d 637, 640 (Cal. 1985) (stating that "a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and its simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device").

361. *See* Winters (1992), *supra* note 11, at 125.

362. *See Walker*, 911 F.2d at 1578-79.

The critical inquiry in *Flanagan* thus should have been not whether the employees had a general expectation of privacy, but whether the employees expected that their employer would intercept, print, and read their E-mail communications.[363] The employees could further argue that their privacy expectations were objectively reasonable because, to their knowledge, their supervisors were not authorized to monitor the E-mail messages.[364]

Second, the *Flanagan* court incorrectly interpreted *Ribas v. Clark* as supporting the conclusion that E-mail is not protected under section 631. In *Ribas*, the California Supreme Court analyzed the legislative history of section 631 and broadly interpreted the section to cover "far more than illicit wiretapping."[365] The court specifically held that section 631 prohibits "willful attempts to learn of the contents of communication in transit" and "attempts to use or publicize information obtained in [that] manner."[366] These expansive prohibitions are not limited to wiretapping per se, and the court could have interpreted Epson's E-mail interceptions in *Flanagan* and *Shoars* to fall under either proscription. The Epson supervisor clearly intended to learn the contents of the employees' messages, and he used the information by firing Shoars.[367]

Third, the *Flanagan* court's contention that the provider exception in the ECPA supported its interpretation of section 631 is both speculative and arguably irrelevant. No court has explicitly applied the provider exception to employer E-mail monitoring, and the extent to which private employer-providers are exempted by the exception is uncertain.[368] Furthermore, no ECPA language equates an employer with a provider, and it seems clear that the exception only pertains to the entity that actually owns and provides the communication service. An employer that subscribes to a common-carrier E-mail service would thus not be the provider of the service.[369] Additionally, the provider exception only

---

363. *See* Winters (1992), *supra* note 11, at 125.

364. *See id.* Defendant Epson could counter these arguments by asserting that the ECPA analysis from *Walker* is inapposite to Epson's intrusion, which was related to work. *Id.* at 126.

365. *Ribas*, 696 P.2d at 640. The *Ribas* court reasoned: "In enacting [section 631], the Legislature declared in broad terms its intent 'to protect the right of privacy of the people of this state' from what it perceived as 'a serious threat to the free exercise of personal liberties [that] cannot be tolerated in a free and civilized society.'" *Id.* at 639-40 (quoting CAL. PENAL CODE § 630).

366. *Id.* at 640.

367. Winters (1992), *supra* note 11, at 126-27.

368. *See supra* notes 94-126 and accompanying text.

369. *See* Winters (1992), *supra* note 11, at 128.

applies when the interception was authorized and the Epson supervisor may not have been authorized to conduct the extensive interceptions at issue in the case.[370] Most importantly, even if the ECPA provider exception would exempt Epson's actions, the legislative history behind the ECPA does not clearly evidence a congressional intent to preempt more protective state laws; states are therefore free to provide stricter privacy protection than that available under federal law.[371]

In the end, the decision by the *Flanagan* court not to extend section 631 protection may simply have turned on the fact that the statute did not specifically include "electronic communications" or "electronic mail" in its coverage. Other state courts may similarly be wary of extending state wiretapping protections to electronic communications without explicit statutory authorization if they recognize parallel inadequacies in their state statutes and pre-ECPA federal law. As in *Flanagan*, the courts may reason that the state legislature, not the courts, should extend the statute's protections to electronic communications.[372] Congress, however, did not amend Title III until technological advancements made the statute obsolete;[373] thus, state courts should not feel constrained by the lethargic federal action in the communications privacy area, especially if the legislative intent behind the state statute supports its application to E-mail.[374] Also, by deferring to state legislatures, courts avoid analyzing the privacy interests at stake and effectively resolve the issue in favor of employers.[375] Such restraint may actually contradict the broad legislative intent behind state wiretapping statutes such as California's section 631.[376]

In the face of technological developments, some states have passed new legislation protecting employees from electronic interceptions and electronic monitoring. In June 1994, the New Jersey legislature extended the coverage of its Wiretapping and Electronic Surveillance Act. The Act

---

370. Although the *Flanagan* complaint asserted that the supervisor had tapped the E-mail lines with the knowledge of Epson, Flanagan v. Epson Am., Inc., No. BC007036, slip op. at 2 (Cal. Super. Ct. Jan. 4, 1991), the conduct may not have been "authorized," given Epson's representations that employee E-mail messages would be confidential. Winters (1992), *supra* note 11, at 127-28.

371. Winters (1992), *supra* note 11, at 127.

372. *See* Baumhart, *supra* note 45, at 946 n.138.

373. Russell S. Burnside, *The Electronic Communications Privacy Act of 1986: The Challenge of Applying Ambiguous Statutory Language to Intricate Telecommunication Technologies*, 13 RUTGERS COMPUTER & TECH. L.J. 451, 455 (1987).

374. *See* Winters (1992), *supra* note 11, at 128-29.

375. *Id.*

376. *See* CAL. PENAL CODE § 630 (West 1988) (providing a broad statement of legislative intent).

was scheduled to remain in effect until July 1, 1994, but the legislature extended its coverage to July 1, 1999.[377] Unlike California's statute, the New Jersey statute explicitly defines "electronic communication."[378] Similar to the ECPA, the statute both criminalizes the interception of an electronic communication and the disclosure and use of an intercepted communication.[379] Additionally, Connecticut and Nevada have increased employee privacy protection by passing laws that restrict the electronic surveillance of employees,[380] but the protection afforded to E-mail communications in these state statutes is uncertain.[381]

Despite these advances in a few states, the attractiveness of arguments advocating expansive state court interpretations remains questionable given the textual omission of privacy protection for electronic communications in many state statutes. Indeed, the fact that a case in California, the "model" state for E-mail protection,[382] denied an E-mail interception claim does not bode well for future employee privacy claims in other states. Moreover, even if courts apply existing state statutes to E-mail interception and accession, the statutes retain important exceptions to liability that, as in the ECPA context, present escape routes for employers who confront potential liability.[383] For instance, Nebraska's general wiretapping statute provides a broad exception specifically allowing an "employer" to "intercept, disclose, or use" an electronic communication "in the normal course of . . . employment."[384] Additionally, the all-party consent requirement in some state statutes will not adequately safeguard E-mail transmissions between employees because both employees are presumably on notice of employer interceptions if the employer publishes a monitoring policy. At best, relying on state statutes to supplement

---

377. 1994 N.J. Session Law Serv. 55 (West).

378. N.J. REV. STAT. § 2A:156A-2m (1993).

379. N.J. REV. STAT. § 2A:156A-3 (1993).

380. Connecticut's statute prevents electronic surveillance of areas provided for the "health or personal comfort of employees or for safeguarding of their possessions." CONN. GEN. STAT. ANN. § 31-48b(b) (West 1987). Prior notification does not constitute an exception under the statute. *See* Lee, *supra* note 25, at 160 n.118. Nevada's statute prohibits the surreptitious monitoring of private conversations. NEV. REV. STAT. ANN. § 200.650 (Michie 1992).

381. *See* Lee, *supra* note 25, at 160.

382. Slind-Flor, *supra* note 291, at 22 (statement of Robert Ellis Smith, editor of the *Privacy Journal*).

383. *See* Lee, *supra* note 25, at 175 (Table 2) (listing state statutes that contain consent and business use exceptions).

384. NEB. REV. STAT. § 86-702(2)(A) (1987).

ECPA protection represents an unacceptable piecemeal response to a privacy problem that demands a comprehensive solution.

III. REMEDY FOR THE FUTURE

Despite the presence of privacy protections through federal statutory law, tort law, and state constitutional and statutory law, no legal source adequately protects private employees' privacy interests in their workplace E-mail communications.[385] Judicial interpretation of the privacy rights of private parties is generally affected by Supreme Court Fourth Amendment law, which does not neatly apply to E-mail and other computer privacy issues.[386] Drawing from this Fourth Amendment jurisprudence, courts construe all four sources of law as holding that a person's right to privacy is violated only when the person has a reasonable expectation of privacy.[387] They implicitly, if not explicitly, require this expectation even though some statutory sources, such as the ECPA, protect communications notwithstanding the presence of any privacy expectation.[388] This emphasis on employee privacy expectations is misplaced because employers can manipulate employee expectations simply by modifying the particulars of the work environment.

Additionally, across these four sources of law, courts balance the interests of employers and employees to determine whether an illegal privacy invasion has occurred.[389] The benefit of such judicial balancing is that it requires courts to analyze the needs and interests of the parties in articulating rationales for favoring one interest over another.[390] As the analysis of the legal sources demonstrates, however, courts have been reluctant to protect employees' privacy interests because their interests often clash with the employer's interest in monitoring and efficiently

---

385. Winters (1992), *supra* note 11, at 94-95.

386. *Id.* at 95.

387. *Id.* (citing, *inter alia*, Schowengerdt v. General Dynamics Corp., 823 F.2d 1328, 1333 (9th Cir. 1987)). The analysis is similar in both the public and private scenarios. *Id.*

388. *See supra* notes 62-65 and accompanying text.

389. *See* Winters (1992), *supra* note 11, at 95-96. *Cf.* Griffin, *supra* note 3, at 524-25.

390. Winters (1992), *supra* note 11, at 96. Commentators have asserted that judicial balancing should accomplish three goals: "(1) to justify the appropriate level of generality for the issues before the court; (2) to insure that the result is based on an adequate factual background; and (3) to not substitute deference for a cogent analysis of the parties' interests." *Id.* (citing Frank M. Coffin, *Judicial Balancing: The Protean Scales of Justice*, 63 N.Y.U. L. REV. 16, 38 (1988)).

managing the workforce.[391] As the controversy over employee privacy rights escalates, a balance must be reached between employees' right to privacy and employers' need to manage their workforce. Failure to clearly resolve these legal issues will result in perplexity, mistrust, and acrimony between employees and their employers.[392]

A. Employer Monitoring Policies

In response to the current legal sources affecting employee privacy interests in workplace E-mail communications, numerous commentators recommend that employers establish corporate policies addressing E-mail privacy and make certain that employees are informed of these policies.[393] Commentators differ in suggesting how the policies should be limited. For instance, the Electronic Mail Association advises employers to communicate written policies to their employees stating that E-mail should be used only for business purposes and that the employer can access employee E-mail in the course of business.[394] Other commentators add that employers should explicitly reserve a property right in their E-mail system so that they may receive statistical information on the system and

---

391. *See generally* Winters (1992), *supra* note 11, at 95-96 (reasoning that the employer's interests outweigh those of the employee in the Fourth Amendment context and that Fourth Amendment jurisprudence affects the common law).

392. Cavico, *supra* note 9, at 1266.

393. *See, e.g.*, ELECTRONIC MAIL ASSOCIATION, ACCESS TO AND USE AND DISCLOSURE OF ELECTRONIC MAIL ON COMPANY COMPUTER SYSTEMS: A TOOL KIT FOR FORMULATING YOUR COMPANY'S POLICY (1991) (prepared by David A. Johnson and John Podesta) [hereinafter ELECTRONIC MAIL ASSOCIATION]; Metz, *supra* note 2, at 25 (noting that George Trubow, director of John Marshall Law School's Center for Information Technology and Privacy Law, suggests that employers should institute monitoring policies); Fitzpatrick (1992), *supra* note 3, at 1172, 1178 (reasoning that informing employees of a monitoring policy will allow the employer to continue monitoring under the consent exception); Droke, *supra* note 4, at 187-92 (offering specific provisions to include in the employer's policy guidelines so as to control the reasonableness of the employees' privacy expectations); Jenero & Mapes-Riordan, *supra* note 5, at 98; Cavico, *supra* note 9, at 1330-31 (reasoning that such proposals "help the employer fulfill its appropriate function of efficient management without contravening the employee's reasonable expectation of privacy"); Barnett & Makar, *supra* note 17, at 755-56 (stating that employers should develop plans that follow federal and state laws because violations bring employers civil and possibly criminal sanctions as well as damage to public and personnel relations); Kane, *supra* note 27, at 438-39; Baumhart, *supra* note 45, at 947-48 (stating that publishing a clearly-defined E-mail policy, which delineates the company's rights and warns employees that the employer can access any messages at any time, provides adequate protection against employee privacy claims). Michele Kane also asserts that establishing clear policies minimizes unfortunate surprises and potentially avoids negative publicity that might result from an employee's invasion of privacy action. Kane, *supra* note 27, at 438.

394. ELECTRONIC MAIL ASSOCIATION, *supra* note 394.

may access the system to protect corporate interests.[395] Still others suggest that employers should prohibit all personal E-mail messages and explicitly warn employees that the employer reserves the right to access and read E-mail messages to determine if communications are work-related or personal.[396]

Despite their discrepant suggestions for the parameters of corporate E-mail policies, commentators are uniform in their belief that publishing E-mail policies and abiding by their strictures give employers a strong, if not insurmountable, defense against any employee claim relating to E-mail privacy.[397] In the wake of these suggestions, some employers, such as Federal Express, American Airlines, and Pacific Bell, have instituted policies informing their employees that they reserve the right to monitor E-mail communications.[398] Other employers have taken steps to assure employees that their E-mail correspondence will not be monitored or read, in some cases by installing systems that allow only the sender and receiver to read the messages.[399]

Regardless of the specifics in the privacy policies adopted by employers, such self-regulation represents an unacceptable solution in the face of potentially invasive employer practices. First, establishing clear corporate E-mail policies more emphatically protects the interests of the employer than those of the employee. Because the employer is the party with the most control in determining the characteristics of the E-mail system it provides and of the work environment generally,[400] employers can tailor E-mail policies to advance their interests in E-mail communications without necessarily incorporating the desires of employees. Furthermore, although these policies eliminate the surreptitious nature of the monitoring, they compromise employee privacy interests by validating a new avenue by which employers may monitor employees. Moreover, not all employers that use E-mail will develop corporate privacy policies,[401] leaving employees protected from invasions at problematically differing degrees.

---

395. Droke, *supra* note 4, at 187.

396. *See id.*; Cavico, *supra* note 9, at 1330; Baumhart, *supra* note 45, at 947.

397. *See, e.g.*, Jenero & Mapes-Riordan, *supra* note 5, at 98; Baumhart, *supra* note 45, at 947-48; ELECTRONIC MAIL ASSOCIATION, *supra* note 394.

398. Glenn Rifkin, *The Ethics Gap: Despite Growing Attention, Many IS Managers Say, "It's not my job,"* COMPUTERWORLD, Oct. 14, 1991, at 83; *see also* Nash, *supra* note 101, at 7 (describing the policy of Epson Corporation).

399. *See* LaPlante, *supra* note 38, at 66.

400. Droke, *supra* note 4, at 193.

401. *Id.* at 198.

Second, the installation of E-mail policies may actually increase tensions between employers and their employees. E-mail is progressively becoming the preferred mode of communication among employees, and protection against employer interception has thus become increasingly important to employee morale. Employees need some sort of conversational outlet during the workday, and the employment context would become unhealthy if employees were not comfortable freely conversing with one another on the preferred mode of communication.[402] Under a policy prohibiting personal E-mail communications, employees will undoubtedly experience the resentment and dehumanization that monitored employees often experience on the job.[403] In fact, monitoring policies may exacerbate such feelings because the policies sanction potentially invasive monitoring as a normal workplace occurrence.[404] Employees may also experience apprehension or mistrust if they believe that the employer's monitoring is due to a suspicion or belief that the employees are dishonest.[405]

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

---

402. For instance, after the Los Angeles Police Department reprimanded several officers for sending racially and sexually offensive E-mail messages, retired L.A. police captain Diane Harber stated, "I think it's very unhealthy for people not to express themselves in human terms with one another [during the workday]." Keubelbeck, *supra* note 24, at E1.

403. *See infra* notes 494-95 and accompanying text; *see also* UNIVERSITY OF WISCONSIN-MADISON, DEPARTMENT OF INDUSTRIAL ENGINEERING & THE COMMUNICATIONS WORKERS OF AMERICA, ELECTRONIC PERFORMANCE MONITORING AND JOB STRESS IN TELECOMMUNICATIONS JOBS 7 (1990) (finding that "electronic monitoring has adverse effects on employees' perceptions of how stressful their jobs are and on their reported levels of physical and psychological strain"); Metz, *supra* note 2, at 25; DeBenedictis, *supra* note 353, at 27 (quoting Michael Baum as stating that invasive monitoring policies will hurt the employer). Moreover, such a policy will likely be ineffective because many employees will continue to send personal messages over the office system. *See* Kane, *supra* note 27, at 439.

404. *See* Winters (1992), *supra* note 11, at 105 n.97.

405. Cavico, *supra* note 9, at 1300 n.177; *see also* Shoop, *supra* note 6, at 13; Piller, *supra* note 7, at 122. For instance, Cindia Cameron of 9 to 5, the National Association of Working Women, states, "People say they feel [electronic monitoring] sets up an atmosphere of suspicion or distrust [because] someone is constantly looking over their shoulder. It feels like spying." Shoop, *supra* note 6, at 13.

interests they value. Indeed, a traditional critique of workplace privacy views conflicts over privacy as emanating from the fact that most applicants are uninformed of potential privacy issues in the workplace and consequently do not seek to bargain with their employer on such issues.[406] 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 the working conditions in their employment positions.[407] Most applicants must adhere to the employer's unilateral terms or they will not be hired,[408] and the continued expansion of E-mail monitoring[409] means that many applicants must consent to being monitored in order to gain employment. Because an employer can generally terminate an at-will employee who objects to employer practices,[410] employees also do not gain a significant new-found bargaining position with the employer when they are hired. Especially considering the recent decline in the percentage of employees involved in collective bargaining,[411] employees today often must either accept the employer monitoring, protest and face possible termination, or voluntarily terminate employment.[412]

Moreover, even assuming that applicants and employees have equal bargaining power with employers, requiring employers to disclose their

---

406. Droke, *supra* note 4, at 167. From this position, some federal courts have barred employee privacy claims, reasoning that workplace privacy should be left to collective bargaining. *See Courts Apply Broad Preemption Test to Emotional Distress, Privacy Claims*, Wash. Insider (BNA) (July 14, 1992).

407. Decker, *supra* note 13, at 563; *see also* David Neil King, *Privacy Issues in the Private Sector Workplace: Protection from Electronic Surveillance and the Emerging "Privacy Gap,"* 67 S. CAL. L. REV. 441, 448 & n.33 (1994).

408. Decker, *supra* note 13, at 563.

409. *See* Metz, *supra* note 2, at 23 (noting that the growing use of E-mail has prompted concerns over confidentiality and that such anxieties have encouraged E-mail monitoring).

410. *E.g.*, Hollenbaugh v. Carnegie Free Library, 436 F. Supp. 1328, 1333-34 (W.D. Pa. 1977) (holding that the termination of an at-will employee discovered to be living with someone in "open-adultery" did not contravene the employee's constitutional right of privacy).

411. *See* Katherine Van Wezel Stone, *The Legacy of Industrial Pluralism: The Tension Between Individual Employment Rights and the New Deal Collective Bargaining System*, 59 U. CHI. L. REV. 575, 578 (1992) (reporting that union membership declined from almost 25% of the nonagricultural workforce in 1980 to less than 17% in 1990). Stone also notes that this decline in the influence of collective bargaining has accompanied an increase in the legally enforceable employment rights for individual employees. *Id.* at 576.

412. Decker, *supra* note 13, at 563. Under the traditional doctrine of at-will employment, employees have the right to terminate employment voluntarily, which theoretically counterbalances the employer's ability to terminate the employee for no justifiable reason.

E-mail monitoring policies merely commodifies employee privacy rights and does not guarantee protection important privacy interests. First, the commodification may often not achieve results that maximize employees' utility because privacy is far less tangible than other interests and is therefore more difficult to quantify in comparing the costs and benefits of a particular work environment.[413] More importantly, as discussed below, privacy rights hinge on important notions of human dignity, and significant privacy interests should therefore not be bargained for and exchanged like chattel. Free-market advocates might respond that denying employers and employees the ability to bargain over certain privacy rights is paternalistic and irrational because intelligent bargaining leads to rational and efficient results.[414] However, our society has customarily regulated behavior seemingly rational under market forces when the behavior was repugnant to the fundamental rights in a civilized society.[415] Employee privacy rights are fundamental rights that should be protected irrespective of market dynamics.

B. Need for New Legislation

Given the inability of employer E-mail monitoring policies to safeguard employee privacy interests, the potential for abusive privacy invasions mandates concerted, systemic redress. In the context of electronic monitoring generally, Congress responded by proposing the Privacy for Consumers and Workers Act ("PCWA").[416] Versions of the

---

413. *See* King, *supra* note 408, at 449.

414. *See id.* at 448 & n.31.

415. For instance, constitutional and statutory restrictions prohibit various forms of employment discrimination irrespective of market forces. *See, e.g.*, Title VII of the Civil Rights Act of 1964, as amended, 42 U.S.C. § 2000e *et seq.* (1988 & Supp. 1993).

416. H.R. 1900, 103d Cong., 1st Sess. (1993) [hereinafter H.R. 1900] (Sept. 15, 1993 version); S. 984, 103d Cong., 1st Sess. (1993) [hereinafter S. 984] (May 21, 1993 version); *see also* Metz, *supra* note 2, at 26-28; Jenero & Mapes-Riordan, *supra* note 5, at 95-96 (both describing the general provisions of the Act). The bill was introduced in the House by Rep. Pat Williams (D-Mont.) on April 28, 1993, and in the Senate by Sen. Paul Simon (D-Ill.) on May 19, 1993. Senator Dale Bumpers (D-Ark.) introduced another bill affecting electronic monitoring on February 4, 1993. The bill, entitled the Telephone Privacy Act of 1993, made lawful the interception of oral or wire communications where all parties consent to the interception or where the interceptor is an employer engaged in electronic monitoring of its employees' communications in the course of the employees' duties. S. 311, 103d Cong., 1st Sess. (1993). In contrast to the PCWA, the bill gained little media attention and little support from other Senators. The bill died in the Senate Judiciary Committee at the end of the 103d Congress. *See* Bill Tracking Report for 1993 S. 311, LEXIS, Legis library, Blt103 file. As of April 24, 1995, the bill had not been reintroduced in the 104th Congress. Search of LEXIS, Legis library, Bltrck file (Apr. 24, 1995).

PCWA were introduced in both the House and Senate, but neither chamber passed its respective version of the bill by the end of the 103d Congress.[417] If the bill is reintroduced in the 104th Congress,[418] the existing versions of the PCWA do not represent a promising avenue for E-mail protection for several reasons. First, although the House bill supplements ECPA protections for E-mail, the Senate version specifically excludes "the interception of wire, electronic, or oral communications as described in [the ECPA]," and thus E-mail, from its definition of "electronic monitoring."[419] Second, both the House and Senate versions permit specific levels of monitoring depending on the employee's length of service.[420] Although the standards work to increase employee privacy, they place unnecessarily unbending obligations on employers that frustrate the ability of employers to engage in monitoring in a manner best suited to the employer's particular business context.

Third, and most importantly, existing versions of the PCWA do not adequately protect E-mail privacy because they eliminate the surreptitious nature of employer monitoring without effectively restricting the scope of the monitoring.[421] Under the PCWA, employers are obliged to notify employees of monitoring practices but they still remain free to monitor the content of work-related E-mail messages[422] of employees with less

---

417. At the end of the 103d Congress, H.R. 1900 had stalled in the House Education and Labor Committee, and S. 984 had stalled in the Senate Subcommittee on Employment and Productivity. *See* Bill Tracking Report for 1993 H.R. 1900, LEXIS, Legis library, Blt103 file; Bill Tracking Report for 1993 S. 984, LEXIS, Legis library, Blt103 file.

418. The bill had yet to be reintroduced in the 104th Congress by April 24, 1995. Search of LEXIS, Legis library, Blttrck file (Apr. 24, 1995).

419. S. 984, *supra* note 417, § 2(2)(C); H.R. 1900, *supra* note 417, §§ 2, 3 (Feb. 23, 1994 version), *analyzed in Section by Section Analysis of the Substitute Privacy for Consumers and Workers Act (H.R. 1900)*, DAILY LAB. REP., Feb. 24, 1994, at d32 [hereinafter *H.R. 1900 Analysis*]. The February 23, 1994 version provides that compliance with the PCWA does not relieve an employer from complying with Title III and the ECPA. *See H.R. 1900 Analysis*, *supra*, at d32.

420. *See H.R. 1900 Analysis*, *supra* note 420, at d32; S. 984, *supra* note 417, § 5(B). As an example of the provisions' unbending nature, the Senate version completely bans random and periodic monitoring of employees with more than five years of service. *See* S. 984, *supra* note 417, § 5(B)(3). In contrast, the House version prescribes specific conditions constituting a "bona fide service observation program" and limits the employer to 15 service observations on employees with more than two years service. *See H.R. 1900 Analysis*, *supra* note 420, at d32.

421. *See* Griffin, *supra* note 3, at 524-25; *see also* Jeffrey S. Kingston & Gregory L. Lippetz, *E-mail Privacy Rights Can Be Tricky, So Firms Need to Study Up*, BUS. J., Feb. 1, 1993, at 21.

422. Both the House and Senate versions state that "no employer may intentionally collect personal data about an employee through electronic monitoring if the data are not confined to the employee's work." H.R. 1900, *supra* note 417, § 9(a)(1) (Sept. 15, 1993 version); S. 984, *supra* note 417, § 10(a).

than five years of service in the Senate version,[423] and of all employees in the House version.[424] As discussed above, simply notifying employees of potential monitoring does not alleviate the privacy burden of intrusive employer practices because most employees do not bargain for their employment and must either accept their employment conditions or risk termination.[425] Furthermore, allowing the monitoring of work-related communications implicates the same problems as in applying the content approach to the ECPA because employers remain free to monitor all communications, at least to determine whether they are business or personal, and because courts must undertake the difficult task of determining which communications are sufficiently work-related.[426] Ironically, the PCWA thus effectively validates the employer's ability to conduct intrusive monitoring practices and further insulates employers from liability under the law.[427]

Given the deficiencies in the PCWA, the most promising strategy to address the need to protect workplace E-mail privacy is further legislative response.[428] Although courts have demonstrated great ingenuity in developing the common law to address changing societal needs,[429] judicial extension of the common law right of privacy would require a fundamental reworking of current conceptions so as to require a near abandonment of common law precedent.[430] Moreover, such judicial activism would be piecemeal, and the costs of litigation might deter employees from bringing claims, especially if punitive damages were not available.[431] A judicial solution therefore could offer neither the uniformity nor the extensive enforcement mechanisms of a well-drafted federal statute.[432]

---

423. *See* S. 984, *supra* note 417, § 5(B)(3).

424. *See H.R. 1900 Analysis*, *supra* note 420, at d32.

425. *See supra* notes 407-16 and accompanying text.

426. *See supra* notes 167-72 and accompanying text.

427. Griffin, *supra* note 3, at 524-25. For more discussion of the PCWA, see Metz, *supra* note 2, at 26-28.

428. *See* Metz, *supra* note 2, at 26; Note, *supra* note 3, at 1913; Droke, *supra* note 4, at 194-98 (proposing a model E-mail statute). As an alternative to further legislation, Michael Droke proposes that the burden of proof should be shifted in the ECPA so that E-mail communications would be presumed private unless proven otherwise. *See* Droke, *supra* note 4, at 193-94. Although such an interpretation would undoubtedly aid employees in pursuing private causes of action against their employers, the approach neglects the need to rethink the right to privacy as being a protection for human dignity. *See infra* part IV.C.

429. Jenero & Mapes-Riordan, *supra* note 5, at 97.

430. Note, *supra* note 3, at 1914 (citing Comment, *Employee Privacy Rights: A Proposal*, 47 FORDHAM L. REV. 155, 181 (1978)).

431. *Id.* at 1915.

432. *Id.*

In addressing the need for further legislative action, a federal response is more desirable than state action. First, state legislation would be insufficient because only federal legislation can address E-mail communications that cross state lines.[433] Second, state legislation, as well as state constitutional amendments, could not guarantee employees in all states a uniform level of protection.[434] Third, state legislative efforts are more likely to be undermined by the apparent ability of prominent corporations to stymie state legislation that strengthens protections for employee privacy interests.[435] For instance, state legislation concerning electronic workplace monitoring has been blocked in Massachusetts and amended in West Virginia after corporations threatened to relocate to other states.[436] More recently, Georgia and New York failed to enact electronic monitoring legislation pending at the end of the 1994 legislative term.[437] In 1995, Georgia introduced new wiretap legislation, and New York introduced new legislation concerning employee electronic monitoring.[438] Both bills are, at the time of this writing, in committee.[439]

C. Rethinking the Right to Privacy

In the call for further federal action, new legislation will not produce lasting change unless it abandons the recent emphasis on the employee's expectation of privacy and on the employer's business interests in monitoring. Indeed, this emphasis essentially guarantees no absolute protection for employees because employees' expectations are increasingly

---

433. Lee, *supra* note 25, at 170.

434. *See* Griffin, *supra* note 3, at 520-21.

435. *Id.* at 520.

436. Furfaro & Josephson, *supra* note 89, at 4. Similar events occurred in New Hampshire. *See* Metz, *supra* note 2, at 27. In 1995, Massachusetts introduced new legislation concerning workplace electronic monitoring, and the bill is currently in committee. *See* Bill Tracking Report for 1995 MA H.B. 2518, LEXIS, Legis library, Matrck file (Apr. 24, 1995).

437. *See* Lee, *supra* note 25, at 160-61; Bill Tracking Report for 1994 GA S.B. 646, LEXIS, Legis library, Trck94 file; Bill Tracking Report for 1994 NY A.B. 10705, LEXIS, Legis library, Trck94 file.

438. 1995 GA S.B. 74 (providing that it shall be unlawful for a person who is a party to any oral, wire, or electronic communication to intercept that communication without the prior consent of the other party) (introduced Jan. 12, 1995); 1995 NY A.B. 2019 (prohibiting employers from monitoring non work-related activities) (introduced Jan. 26, 1995).

439. *See* Bill Tracking Report for 1995 GA S.B. 74, LEXIS, Legis library, Gatrck file (Apr. 24, 1995) (stating that a substitute bill has passed the Georgia Senate and is now in the Georgia House Committee on Judiciary); Bill Tracking Report for 1995 NY A.B. 2019, LEXIS, Legis library, Nytrck file (Apr. 24, 1995).

compromised by developing technology, newly conceived employer interests, and expansive employer monitoring policies. In order to provide absolute and substantive protection to employee privacy interests and rectify current shortcomings in common law, constitutional, and statutory approaches, the principles underlying the right to privacy must be reconsidered.[440] In the tradition of Professor Edward Bloustein, privacy must be reconceived as an independent right based on human dignity and respect for individuals.

The current emphasis on the balancing of interests can be traced to a 1960 law review article by Dean William Prosser, in which Prosser suggested that privacy is not an independent value but is rather a composite of interests in reputation, emotional tranquility, and intangible property.[441] In a 1964 response, Bloustein rejected Prosser's prevailing view. Bloustein argued that Prosser's analysis reduces the unique right to privacy to a mere application in novel contexts of the traditional legal doctrines of infliction of mental distress, defamation, and misappropriation, which are all designed to protect well-identified and established social values.[442] This reduction, Bloustein continued, conflicted with the original conception of privacy described by Samuel D. Warren and Louis D. Brandeis, who believed that the mental distress resulting from a privacy intrusion is not what makes the act wrongful, but that the distress is a byproduct of the independent tort, the invasion of privacy.[443]

Bloustein demonstrated his belief in an independent notion of privacy by analyzing intrusion into seclusion cases to conclude that mental distress was not the gravamen in any of the cases.[444] He further distinguished the intrusion cases from cases concerning the tort of intentional infliction of

---

440. *See* Note, *supra* note 3, at 1914.

441. William Prosser, *Privacy*, 48 CAL. L. REV. 383, 392, 422 (1960).

442. Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 965-66 (1964) [hereinafter Bloustein, *Human Dignity*].

443. Bloustein, *Human Dignity*, *supra* note 443, at 967 (citing Warren & Brandeis, *supra* note 186, at 197-98, 213). Bloustein added that because Warren and Brandeis were less successful in describing the interest violated by an invasion of privacy than they were in describing what it was not, Prosser and other theorists subsequently predicated the privacy right on bases actually rejected by Warren and Brandeis. *Id.* at 970 (citing HARPER & JAMES, TORTS § 9.6 (1956); RESTATEMENT OF TORTS § 867 (1939)).

444. *Id.* at 972 (citing Prosser, *supra* note 442, at 422). Bloustein added that, in most instances, the lines of authority relied upon in the intrusion cases are significantly different from those relied upon in the cases concerning the intentional infliction of emotional distress. *Id.*

cases, required "severe emotional distress" as a requisite element of the cause of action.[445] In his primary disagreement with Prosser, Bloustein emphasized the traditional conception of the right to privacy as a "spiritual" value,[446] which includes the "right to be left alone" [447] and which "posit[s] the individual's independence, dignity, and integrity."[448] He argued that in cases of intrusion into privacy, the core of the invasion is a "blow to human dignity, an assault on human personality."[449]

Bloustein analogized this conception of privacy to the constitutional notion of unreasonable search and seizure. He reasoned that the Fourth Amendment recognizes the intrusion as unlawful because it involves a violation of the constitutionally protected liberty of the person, a liberty the Supreme Court has called "basic to a free society."[450] Although the Fourth Amendment and tort law are obviously distinguished by their application to different intruders, Bloustein found that "a similar wrong is perpetrated in both instances."[451] Indeed, he argued that this preservation of individual human dignity is the common thread linking tort cases to other forms of legal protection of privacy, including wiretapping and eavesdropping statutes, none of which predicate recovery upon a showing of mental distress.[452]

In a 1978 article, Bloustein addressed Judge Richard Posner's economic theory of privacy, which viewed privacy as an instrumental value based on the concealment of personal information.[453] Bloustein responded by recognizing that privacy is so integrally and inextricably linked to personal dignity that it remains an "ultimate" or "final" value of tremendous social importance. He asserted that privacy is a personal value, which is incapable of exchange.[454]

---

445. *Id.* at 973 (citing, inter alia, William Prosser, *Insult and Outrage*, 44 CAL. L. REV. 40, 43 (1956)).

446. *Id.* at 971 (analyzing Warren & Brandeis, *supra* note 186, at 197).

447. *Id.* at 970 (analyzing Warren & Brandeis, *supra* note 186, at 195).

448. *Id.* at 971.

449. *Id.* at 974.

450. *Id.* at 975 (quoting Wolf v. Colorado, 338 U.S. 25, 27 (1949)).

451. *Id.* at 975, 994. Bloustein continued comparing the Fourth Amendment to the tort invasion of privacy by describing the similarities between Brandeis' original 1890 law review article and his dissent in Olmstead v. United States, 277 U.S. 438 (1928), in which Brandeis evidenced his increasing concern about the evils of unbridled intrusion upon private affairs. Bloustein, *Human Dignity*, *supra* note 443, at 975-77.

452. Bloustein, *Human Dignity*, *supra* note 443, at 994-97, 1000-01.

453. Edward J. Bloustein, *Privacy Is Dear at Any Price: A Response to Professor Posner's Economic Theory*, 12 GA. L. REV. 429, 436-39 (1978) (citing Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393 (1978)).

454. *Id.* at 442-47 .

The effects of Bloustein's scholarship are apparent in the commendation current privacy scholars have given his theories. For instance, Professor Sheldon W. Halpern has recently written:

> It is . . . as a grand moral statement that Bloustein's work will endure; and it is within the context of that moral statement that the law's response must be measured. By his continuing efforts to illuminate the moral code of the right of privacy, Bloustein ultimately kept the issue [of the meaning of privacy] from deteriorating into semantic quibbling. That effort requires us, today, to confront the moral issues surrounding the problem of protecting human dignity. . . .
>
> If Prosser's analytic dissection was an attempt to define and rationalize the body of the right of privacy, Bloustein sought its soul.[455]

Commentators who do not directly cite Bloustein's theories also demonstrate the importance of his conceptions by their emphasis on privacy as linked to human dignity.[456] Recent judicial opinions similarly recognize this conception of privacy. For instance, as recently as in the 1994 case *Hill v. National Collegiate Athletic Ass'n*, the California Supreme Court reasoned that privacy rights "have psychological foundations emanating from personal needs to establish and maintain identity and self-esteem by controlling self-disclosure."[457] Regarding privacy conceptions in constitutions, commentators have further asserted that the California Constitution rejects Prosser's conception of privacy and embraces the notion of privacy as a fundamental right protecting human dignity.[458]

Bloustein's conception of privacy also parallels ethical obligations under which modern theorists have called employers to "respect their employees [sic] personal dignity and integrity by allowing them sufficient autonomy to function without constant and ubiquitous supervision and

---

455. Sheldon W. Halpern, *Rethinking the Right of Privacy: Dignity, Decency, and the Law's Limitations*, 43 RUTGERS L. REV. 539, 544 (1991).

456. *See, e.g.*, Winters (1992), *supra* note 11, at 106-07 (reasoning that legal decisions allowing intrusive employer monitoring are damaging because they fail to consider the employee's personal dignity).

457. 865 P.2d 633, 647 (Cal. 1994).

458. *E.g.*, Heredia, *supra* note 3, at 328.

inspection of their work and personal lives."[459] Theorists assert that employers maintain a moral responsibility to respect the privacy interests of employees based on the American legal notion that corporations enjoy the legal privileges and obligations attributed to natural persons in our society.[460] As corporations enjoy privacy safeguards as citizens, they can therefore logically be expected to respect the privacy interests of their employees.[461] Moral theorists distinguish legal and ethical obligations,[462] but Bloustein's conception unites the two, giving legal force to the ethical obligations which modern theorists recognize are crucial to combating privacy invasions in the private employment context.[463]

Applying Bloustein's conception of privacy to the current legal doctrines affecting workplace E-mail privacy underscores the existing deficiencies in employee protection. With this conception, the employee's interest in individual human dignity appears newly solidified against the encroaching business interests favoring privacy intrusions. In his 1964 article, Bloustein specifically predicted that the identification of the social value of privacy would shape the legal system's approach to electronic eavesdropping, which already had begun to threaten the human dignity values underlying the right to privacy.[464] Although the incorporation of his privacy conception fundamentally alters the balance between the employer and employee interests at stake, his conception does not remove the scales. Indeed, Bloustein recognized that all privacy invasions will not warrant liability because certain invasions will be excused by competing public policies or social interests.[465] He nevertheless asserted that rethinking the privacy interest undeniably affects the nature of the cause of action and the available defenses because the interest enters into the complex process of balancing conflicting social values, which courts undertake in developing new remedies.[466]

---

459. Cavico, *supra* note 9, at 1345.

460. *See* Linowes & Spencer, *supra* note 2, at 613-14.

461. *See id.* at 614 (citing ROBERT HESSEN, IN DEFENSE OF THE CORPORATION 84-85 (1979)).

462. *See, e.g.*, Cavico, *supra* note 9, at 1344-46; Halpern, *supra* note 451, at 560-63.

463. *See, e.g.*, Cavico, *supra* note 9, at 1345 ("While employees seek legal redress through the appropriate privacy tort, moral pressure also emerges as an available and persuasive method to combat invasions of privacy in the private employment sector.").

464. Bloustein, *Human Dignity*, *supra* note 443, at 1005-06.

465. *Id.* at 1004.

466. *Id.* at 1005.

D. Statutory Proposal

From this reaffirmed emphasis on the importance of privacy, a new federal statute governing workplace E-mail communications principally should establish the "compelling business interest" standard as the required justification employers must satisfy in order to intercept or access the content of any employee E-mail communication transmitted through any network operated on the employers' premises.[467] Employers would remain free to monitor the transactional information concerning E-mail messages (such as the sender, receiver, subject heading, and number of messages sent) under the traditional tort standard, which balances the legitimate business interests of the employer against the employee's reasonable privacy interests. The new federal statute should also specify that the employer must demonstrate a compelling business interest each time it intercepts or accesses a communication, without reference to the employee privacy expectations in the E-mail communications.[468] With such explicit statutory language, employers will not be able to continue abusive privacy intrusions simply by minimizing employee privacy expectations to the point where courts might consider no privacy interest as having been invaded in the first place.

In establishing the compelling business interest standard, the statute would imply that courts should apply the new standard as they historically have applied the "compelling governmental interest" standard in federal constitutional privacy jurisprudence.[469] The standard would thus require the employer to demonstrate that the E-mail monitoring was the "least restrictive alternative" furthering the employer's business interests. Furthermore, deducing the confines of the standard from federal constitutional law would prevent the standard from being an impenetrable barrier for employers. For instance, relatively recent Supreme Court

---

467. *Cf.* Heredia, *supra* note 3, at 325-27 (arguing, before the *Hill* decision, that a compelling interest should be required to justify infringement of an employee's or applicant's right to privacy). This standard would include networks that the employers own and manage as well as common-carrier networks to which employers subscribe.

468. Importantly, privacy expectations are not relevant to the protection of electronic communications under the ECPA, yet such expectations have affected judicial applications of the ECPA exceptions. *See supra* notes 62-65 and accompanying text. Thus, the statute should unequivocally require employers to demonstrate a compelling interest regardless of the existence of such workplace contextual particulars as employee notice.

469. Although the statute could explicitly delineate that courts look to federal constitutional jurisprudence in applying the standard, such a delineation is likely unnecessary. An extensive analysis of the "compelling interest" standard appears in the various opinions of Hill v. National Collegiate Athletic Ass'n, 865 P.2d 633 (Cal. 1994).

cases such as *National Treasury Employees Union v. Von Raab* have allowed privacy intrusions under the constitutional standard, but only after the government offered such strong compelling interests as protecting public safety and safeguarding national borders.[470] Although the compelling business interest standard would involve the same balancing process as the compelling governmental interest standard, the interests utilized in the equation would be significantly different. Employers would not be required to demonstrate "governmental" interests in E-mail monitoring, but they would be obliged to demonstrate "business" needs that compel the application of E-mail monitoring. The weight of the employer's business needs would depend on a case-by-case analysis of the particulars in the employment context at issue. As an example, an employer may have a compelling need to monitor E-mail content when employees commonly use the medium to communicate with clients, whereas another employer may not have such a need if it solely desires to minimize workplace gossip occurring within a purely intra-office E-mail network.

In contrast to proposing a statute establishing the compelling business interest standard, several commentators have suggested statutes requiring employers to develop monitoring notification procedures.[471] Although notification undoubtedly protects against unexpected intrusions, any legislation relying on employee notice to safeguard employee privacy is sorely deficient because notification alone ultimately serves to institutionalize a marginal view of privacy and legitimize practices that infringe upon human dignity. Imposing the compelling business interest standard on employers, however, recognizes privacy as an important social interest whose value is destroyed if left unregulated in the market. As Bloustein implies, employees who sell their privacy interest in workplace E-mail communications do not actually exchange what had been of value to them. Privacy is of personal value to the employee, and the sale destroys the value.[472] Applying a standard traditionally reserved for governmental intrusions upon fundamental rights also recognizes that private employers are increasingly amassing power that rivals governmental entities. As mentioned above, commentators have noted that computer and electronic

---

470. 489 U.S. 656, 670, 677, 679 (1989) (involving the drug testing of U.S. Customs officials); *see also* Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 628 (1989) (involving the drug testing of railroad employees).

471. *See, e.g.*, Lee, *supra* note 25, at 177.

472. *See* Bloustein, *Human Dignity*, *supra* note 443, at 445.

monitoring intensify employee privacy concerns because such monitoring abolishes the desired balance of power between employees and employers.[473]

The compelling business interest standard also enjoys advantages because it is not an absolute bar to E-mail monitoring in all employment contexts.[474] The standard does allow monitoring in extreme circumstances,[475] thus honoring Bloustein's recognition of the importance of considering whether privacy violations may be justified by competing social values and interests. Furthermore, the balancing inherent in the compelling interest standard differs from the PCWA, which imposes specific uniform obligations that are inflexible and unresponsive to the differences in the various work environments using E-mail.[476] The compelling interest standard, in contrast, presents employers with the legal framework through which employee E-mail privacy will be protected, but it does not require the employer to institute specific practices. Employers remain free to tailor their workplace in the manner that most efficiently protects employee E-mail privacy. Upon addressing a privacy claim, courts could then effectively balance the needs, interests, and limitations of the litigants, taking into account the particular circumstances in the case.[477] This balancing approach utilizes the advantages of case-by-case adjudication, as recognized by Justice O'Connor in her plurality opinion in *O'Connor v. Ortega*.[478] At the same time, it rejects the permissive reasonableness standard in *Ortega* and imposes a more protective compelling interest standard. In the end, the compelling business interest standard effectively fortifies employee

---

473. *See* Linowes & Spencer, *supra* note 2, at 598 (citing Fred Weingarten, *Communications Technology: New Challenges to Privacy*, 21 J. MARSHALL L. REV. 735, 746 (1988)); Griffin, *supra* note 3, at 494; Winters (1992), *supra* note 11, at 96.

474. *But cf.* Rifkin, *supra* note 399 (noting that some advocates believe that E-mail monitoring is wrong in all circumstances).

475. *See, e.g.*, National Treasury Employees Union v. Von Raab, 489 U.S. 656, 677 (1989) (justifying a governmental privacy intrusion because of public safety factors and the need to protect national borders); *see also* White v. Davis, 533 P.2d 222, 234 (Cal. 1975) (stating that the California privacy amendment "does not purport to prohibit all incursion into individual privacy but rather [requires] that any such intervention must be justified by a compelling interest").

476. *See, e.g.*, Lee, *supra* note 25, at 169; *see also* Barnett & Makar, *supra* note 17, at 740 (criticizing the provision in the original version of the PCWA that required employers to provide employees and third parties with beep tones whenever monitoring occurs).

477. *See* Winters (1992), *supra* note 11, at 105-07 (analyzing the benefits of proper judicial balancing).

478. 480 U.S. 709, 717-18 (1987) (plurality opinion).

privacy interests, which are currently protected only through ephemeral expectations continually subject to employer modification.

E. Employer Benefits from Increasing Employee Privacy

Believing that the forces of efficiency run counter to the forces of privacy protection, some critics might argue that implementing a heightened compelling interest standard would serve as yet another unnecessary impediment to the efficient operations of the workplace.[479] However, as David F. Linowes and Ray C. Spencer have noted:

> Nothing can be considered right from the standpoint of efficiency if it is wrong morally. Those who think there is a basic conflict between long-term management effectiveness and safeguarding personal privacy rights must be either inexperienced in the art and science of management or ignorant of the consequences of personal privacy abuses. Full freedom is as necessary to the health and vigor of business as it is to the health and vigor of citizenship.[480]

Indeed, it is far from clear why the goal of an efficient workplace is best achieved through privacy laws that so heavily favor employers. Decisions such as *O'Connor v. Ortega*[481] assume that employers need practically unlimited ability to monitor employees, but substantial evidence suggests that increasing workplace privacy can improve employee productivity.[482] This increase presumably derives both from the dignity and respect employees feel from the knowledge that they are not constantly being monitored[483] and from the fact that employees worry less about identifying a sharp line between their work and personal lives.[484]

---

479. *See* Linowes & Spencer, *supra* note 2, at 619.

480. *Id.*

481. 480 U.S. 709 (1987).

482. *See* Winters (1992), *supra* note 11, at 105, 107 (citing, inter alia, LOUIS HARRIS & ASSOCIATES, INC. & DR. ALAN F. WESTIN, THE DIMENSIONS OF PRIVACY: A NATIONAL OPINION RESEARCH SURVEY OF ATTITUDES TOWARD PRIVACY 32-41 (1981) (reasoning that employers should recognize that employee productivity is linked to workplace privacy)); *see also* Terry M. Dworkin, *Protecting Private Employees from Enhanced Monitoring: Legislative Approaches*, 28 AM. BUS. L.J. 59, 75 n.92 (1990).

483. Winters (1992), *supra* note 11, at 107 (citing *Ortega*, 480 U.S. at 718 (plurality opinion)).

484. *Id.* at 105 (citing Dworkin, *supra* note 483, at 75 n.92).

For example, despite employers' argument that E-mail monitoring increases their ability to ensure that employees work efficiently and productively,[485] the Communications Workers of America has testified before Congress that West Virginia and Wisconsin have experienced no decline in service quality or productivity since the states enacted laws banning workplace telephone monitoring.[486] In fact, West Virginia's C & P Telephone ranked number one of all Bell Telephone Companies in six out of twelve customer service categories.[487] Similarly, officials at Federal Express report that productivity has attained an all-time high since it stopped monitoring individual employees and began surveying work performance of departments as a whole.[488] These reports from individual employers support the findings of the Office of Technology Assessment, which found that the elimination of secret monitoring of telephone operators resulted in improved service quality, fewer customer complaints and employee grievances, a drop in absenteeism, and a reduction in management costs.[489] Other industrialized nations have also recognized that surreptitious monitoring impedes productivity and damages employee morale. Japan, Germany, and Sweden impose tight restrictions on employee monitoring and their service quality and productivity have remained among the best in the world.[490]

The employer who constantly invades its employees' personal privacy "tear[s] apart the fabric of trust and cooperation that binds companies and their employees."[491] Any resulting lack of trust may, in turn, increase monitoring and operating costs.[492] Studies have demonstrated that monitored employees experience tension and anxiety, which may produce a decline in employee productivity and workplace satisfaction[493] as well

---

485. *See* J.W. Waks & C.R. Brewster, *Privacy Bill Targets Work Site Monitoring*, NAT'L L.J., Jan. 18, 1993, at 18-20 (presenting arguments that workplace monitoring is a "valued management tool for measuring employee productivity and performance").

486. PRIVACY TIMES, July 20, 1987; *see also* Julie A. Flanagan, *Restricting Electronic Monitoring in the Private Workplace*, 43 DUKE L.J. 1256, 1275-76 (1994) (stating that AT&T's Hotel Billing Information System in Tempe, Arizona, was rated equal to or better than any other AT&T office even though the Tempe office did not monitor its employees).

487. Fitzpatrick (1992), *supra* note 3, at 1170.

488. *Id.*

489. *See* Flanagan, *supra* note 487, at 1275

490. Fitzpatrick (1992), *supra* note 3, at 1170.

491. Winters (1992), *supra* note 11, at 105 (quoting Caldwell, *supra* note 22, at 34).

492. *Id.* (citing JESSE E. CHOPER ET AL., CASES AND MATERIALS ON CORPORATIONS 25-28 (3d ed. 1989)). One commentator argues that communications monitoring should be avoided because it deters employees from whistle-blowing and from organizing unions. Fitzpatrick (1992), *supra* note 3, at 1170.

493. Ronald E. Roel, *Injured by Big Brother*, NEWSDAY, Oct. 5, 1990, at 49

as an increase in occupational health problems.[494] Furthermore, this perception of mistrust and unfairness resulting from employer monitoring practices may motivate employees to seek union representation.[495] In the end, E-mail monitoring may thus exacerbate the problems it was designed to correct.

Essentially, current workplace privacy law allowing intrusive monitoring casts employers and employees as adversaries and often portrays employees as incapable of managing their given responsibilities and of establishing productive individual work schedules.[496] This adversarial relationship is antithetical to the opinions from various business, labor, and government entities, such as the Department of Labor, which assert that cooperative labor relations are "essential to the future success of the American industry."[497] Business experts, in contrast, argue that successful companies do not treat their employees like enemies but rather offer employees a participatory environment in which they develop personal and professional incentives to work efficiently.[498] Promoting an atmosphere that fosters trust promotes cooperation and teamwork, which further increase employee productivity. Accordingly, many corporations, such as Ford and Motorola, have instituted employee participation programs to boost employee morale and increase employee

---

(discussing a study by the Communications Workers of America and an ergonomics expert, which concluded that electronic monitoring of workers at computer terminals is linked to increased health ailments and to psychological stress); Frank Swoboda, *Study Links Electronic Monitoring, Stress*, WASH. POST, Oct. 14, 1990, at H3 (describing a University of Wisconsin study that found twice as many electronically monitored workers reported wrist pains and 20% more reported neck pains, as compared with those who were not monitored, and that the monitored employees noted higher incidents of depression, tension, anger, and extreme anxiety); Peter Blackman & Barbara Franklin, *Blocking Big Brother: Proposed Law Limits Employers' Right to Snoop*, N.Y. L.J., Aug. 19, 1993, at 5 (citing a Massachusetts survey that reported that 65% of employees at companies monitoring for workplace efficiency could not perform their tasks effectively because they were required to work too quickly); Flanagan, *supra* note 487, at 1263 (discussing a 1991 study by the National Institute for Occupational Safety and Health, which found that heavily monitored clerical workers "exhibited a greater degree of stress, depression, anxiety, instability, fatigue, and anger").

494. *See* Fitzpatrick (1991), *supra* note 8, at 36 (noting that stress-related symptoms among employees have been estimated to cost U.S. businesses $50 to $75 billion annually).

495. *See* Jenero & Mapes-Riordan, *supra* note 5, at 97.

496. *See id.* at 74; Winters (1992), *supra* note 11, at 105.

497. Flanagan, *supra* note 487, at 1276-77 (citing BUREAU OF LABOR-MGMT. RELATIONS & COOPERATIVE PROGRAMS, U.S. DEP'T OF LABOR, FIRST INTERIM REPORT, U.S. LABOR LAW AND THE FUTURE LABOR MANAGEMENT COOPERATION 25 (1987)).

498. Winters (1992), *supra* note 11, at 105-06 (citing, inter alia, ERIC G. FLAMHOLTZ & FELICITAS HINMAN, THE FUTURE DIRECTION OF EMPLOYEE RELATIONS 145-63 (1985)); Piller, *supra* note 7, at 121-22 (quoting Professor Alan F. Westin of Columbia University).

productivity.[499] In sum, employees who have a distinct area of workplace privacy may work more efficiently than employees who are continuously being scrutinized by their employers.[500]

E-mail monitoring may also hurt employers because it discourages employees from using the E-mail service. E-mail is designed as a communications technology,[501] and it requires a degree of confidentiality in order to be used effectively.[502] In the absence of privacy protection, employees will choose alternative forms of communication that receive more significant legal protection from interception.[503] Employees who might be wary of employer monitoring may also hesitate in being completely candid in their E-mail communications. This hesitancy could lead to miscommunication and ill-informed workplace decisionmaking. Creating such a disincentive ultimately disadvantages the employer because employees forego the benefits of using E-mail. These disincentives may especially hurt employers as employees increasingly rely on E-mail as a primary mode of intra-office communication.[504]

Employers may be recognizing the deleterious effects of unrestricted employee monitoring, as a recent survey of nearly 400 employers showed that approximately two-thirds believed monitoring was ineffective or counterproductive.[505] Many of the nation's largest and most progressive corporations have also voluntarily developed workplace policies designed to improve employee privacy and confidentiality.[506] One of these companies, IBM, believes its privacy policies make smart business sense because its actions have boosted employer-employee relations.[507] Other companies, such as US West and Northern Telecom, have voluntarily decided to make electronic monitoring less intrusive after recognizing the

---

499. *See* Flanagan, *supra* note 487, at 1276-77 & nn.145-47 (reviewing employee participation schemes at several companies).

500. Winters (1992), *supra* note 11, at 106.

501. *See* OTA, ELECTRONIC SURVEILLANCE, *supra* note 34, at 45.

502. Griffin, *supra* note 3, at 521-22.

503. *Id.* at 522 (citing, inter alia, 132 CONG. REC. S7991 (daily ed. June 16, 1986) (statement of Sen. Patrick Leahy (D-Vt.))).

504. Winters (1992), *supra* note 11, at 106.

505. Swoboda, *supra* note 494, at H3A (describing a study by the Conference Board, a New York business-oriented research organization).

506. Linowes & Spencer, *supra* note 2, at 619 (describing the development of policies protecting the privacy of personnel records). In addition to IBM and US West, American Express, Citibank, and Equifax describe their electronic monitoring of employees as severely circumscribed. Piller, *supra* note 7, at 122-23.

507. Linowes & Spencer, *supra* note 2, at 619-20. Equitable Life Insurance, Bank of America, and Citibank are other companies that have instituted such policies to protect the confidentiality of personnel records. *Id.*

health risks and job stress that result from such monitoring.[508] However, as the growth of employee privacy concerns demonstrates, such laudable employers represent a limited number of the total American workforce. Thousands of other large, medium, and small employers employing millions of workers have not voluntarily acted to protect employee privacy.[509] While some of these employers may simply not have recognized the economic benefits of protecting employee privacy, other employers are in contexts where the economic considerations do not support limiting employee monitoring in order to increase employee productivity and morale. All employees, however, retain a right to a certain level of workplace privacy, and further federal legislation would thus serve to ensure a uniform level of privacy protection for all employees, whatever the particular rationale of each employer for withholding privacy safeguards.

Some opponents of requiring employers to present a compelling business interest in order to monitor the content of employee E-mail communications may argue that many employers will simply dismantle and cease operating their internal E-mail networks. This argument ignores the substantial evidence cited above demonstrating that increasing employee privacy protections actually increases employee efficiency and productivity.[510] Thus, employers who continue operating their E-mail networks but cease E-mail monitoring may experience efficiency and productivity increases. Moreover, even if employers do experience any decline in efficiency or productivity, they will continue providing E-mail services for two reasons. First, discontinuing E-mail services will destroy the ability to recapture any initial operating costs expended in establishing the network and training employees in how to use the system. Second, and more importantly, employers gain such significant benefits from E-mail networks that these benefits undoubtedly will outweigh any marginal decreases in employee efficiency and productivity that might result from discontinuing E-mail content monitoring.[511] The continued presence of these substantial benefits will similarly cause employers without existing E-mail networks to install such networks even if they sense that an inability to monitor the content of communications may

---

508. Shoop, *supra* note 6, at 14-15; Flanagan, *supra* note 487, at 1281; *see also* Lory Zottola Dix, *Some Organizations Are Defining Mail Privacy*, COMPUTERWORLD, Nov. 23, 1992, at 87 (describing an E-mail policy adopted by some companies).

509. Linowes & Spencer, *supra* note 2, at 620.

510. *See supra* notes 483-90 and accompanying text.

511. *See supra* notes 26-28 and accompanying text.

result in a marginal decrease in efficiency or productivity. In sum, enacting the compelling business interest standard will protect important privacy interests, maintain workplace benefits arising from E-mail communications, and even increase employee efficiency and productivity in many contexts.

CONCLUSION

Each of the sources of law covering E-mail privacy in the workplace provides protection based on balancing the employee's privacy expectation against the employer's business justifications for intruding upon the employee's privacy. As argued, each of these sources remains deficient because it gives the employer the power to determine its liability simply by modifying the work environment to decrease employee privacy expectations. This inadequate protection afforded employee E-mail disregards the important overarching principle that respecting other individuals means, in part, allowing them some minimal level of privacy in order to function with dignity.[512] It is illogical to assert that this minimum level of privacy should vanish when individuals step onto employer premises.[513] Indeed, the need for workplace privacy intensifies upon the recognition that substantial evidence indicates that employees are spending an increasing amount of time in the work environment.[514] Protecting employees, not because their expectations are deemed objectively reasonable, but because their personal dignity is at stake, results in a call for more stringent legal protections of employee privacy.

Stricter federal legislation represents one promising alternative for ensuring that employees obtain adequate privacy protection in their E-mail communications. The debate over E-mail privacy, however, is but one example of the mounting concern over workplace privacy issues surrounding continued innovations in telecommunications and computer technologies. For instance, a recent federal law suit alleging unlawful voice-mail eavesdropping has prompted new concern regarding employer monitoring of employee voice-mail.[515] Due to the ability of these

---

512. See Winters (1992), *supra* note 11, at 107 (citing GEORGE ORWELL, 1984 (1949)).

513. *See* Piller, *supra* note 7, at 123 ("'employees should not be forced to give up their freedom, dignity, or sacrifice their health when they go to work'") (statement of Sen. Paul Simon (D-Ill.)).

514. O'Connor v. Ortega, 480 U.S. 709, 739 (1987) (Blackmun, J., dissenting).

515. *See* Janice Builard, *A Voice-Mail Privacy Suit Is Setting Off Alarm Bells*, NAT'L

technological innovations to promote workplace efficiency and productivity, their development has acquired its own inertia even though employers do not understand the ramifications of that development on employee privacy rights. In addition to the need for new federal legislation, employee E-mail monitoring thus signifies the need for a larger response, a reevaluation of all the effects of the technological revolution on the workplace.

L.J., Feb. 13, 1995, at B1, B2 (reporting on *Huffcut v. McDonald's Corp.*, No. 94-CV-6589 (W.D.N.Y. filed Dec. 7, 1994)).