Reading Your Every Keystroke: Protecting Employee E-mail Privacy

> Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.[1]

INTRODUCTION

Employees in the private workforce currently enjoy no privacy in their electronic mail communications. Legal doctrines, which seem to recognize the right of privacy for employees, have been advocated since 1890 when Warren and Brandeis wrote their seminal article *The Right to Privacy.*[2] Even though there has been a general trend to recognize privacy in various aspects of American life, the courts have been wary to extend that right very far into the workplace. To date, no court has considered the tort of intrusion into seclusion to encompass the right to private e-mail communications in the private workplace.

Employers have begun monitoring their employees e-mail communications in an effort to stem liability for abuses of e-mail. Employers have found that the increasing use of e-mail has increased vulnerability to corporate espionage and liability for fostering a hostile work environment. Employers believe that monitoring is necessary to discourage such activity and to limit their liabilities. Monitoring is detrimental to employee privacy and creates unnecessary stress that has a direct negative impact on employees' emotional and physical health.

Employee privacy is not sufficiently protected by the law. From the free press of the 1800s to the Internet of today, technological advances have increased invasion of personal privacy. Current legislative efforts fall short of adequately protecting employee privacy. The common law fails to recognize such invasions as actionable. New legislation is needed to address employee privacy and the common law should recognize a new tort cause of action for invasion of employee privacy. If the law cannot or will not change to meet these needs, employees need to protect their privacy using encryption technology.

---

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). This article launched the creation of the invasion of privacy tort in American jurisprudence.

2. *Id.*

What is Privacy?

In order to understand what the right to privacy is, one must understand the concept of privacy. Authors cannot seem to agree on any one definition. Warren and Brandeis echo Judge Cooley's definition of "the right to be let alone."[3] Lawrence Lessig supports the notion that privacy is the power of control over personal information and what can become known by others about you.[4] Privacy can also be defined by what it does: it protects our personhood, which we believe must remain sacrosanct.[5] The basic concept of privacy, distilled from these various authors, seems to be the right of the person from whom information is desired to exclude unwanted acquisition of personal information by others.[6]

The constitutionally protected right of privacy was derived from the penumbra of other protections found in the Bill of Rights.[7] Such rights, however, generally cannot be enforced against non-governmental entities. While employees still maintain their Fourth Amendment rights against unreasonable searches and seizures by state actors, these protections do not exist where the alleged infringer is a private actor.[8] To find a remedy for private invasions of privacy, one must turn to common law tort.

HISTORY

A History of the Right of Privacy

The right of privacy in the common law, specifically in tort, had not been eloquently stated until 1890, when Warren and Brandeis assembled a patchwork of cases that seemed to support a notion of a privacy right in the common law.[9] From these cases, Warren and Brandeis developed the first serious discussion of the right of privacy in American jurisprudence. To understand what the right "to be let alone"[10] meant to Warren and Brandeis, one must look at the world in which they lived.

---

3. *Id.* at 195.

4. LAWRENCE LESSIG, CODE 143 (Basic Books 1999).

5. Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737, 739 (1989) (discussing validity of using principle of personhood to explain privacy). "Whatever its genesis, 'personhood' has so invaded privacy doctrine that it now regularly is seen either as the value underlying the right or as a synonym for the right itself." *Id.* at 752.

6. In some respects, this definition parallels the basic concepts of property rights. Lessig discusses the concept of privacy as property in light of attempting to control information. Where such information becomes a commodity, the party that wants the information must ask for it, and the person from whom information is desired must consent, and neither party will be worse off where the trade occurs in the marketplace. *See* LESSIG, *supra* note 4, at 159-62. My construct of privacy stops short of commodifying privacy, but does not prevent such transactions from occurring.

7. *See* Griswold v. Connecticut, 381 U.S. 479 (1965) (finding constitutionally protected right of privacy from the "penumbra" of the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments).

8. *See* U.S. CONST. amends. IV & XIV; Burton v. Wilmington Parking Auth., 365 U.S. 715 (1961) (finding symbiotic relationship between state and private business sufficient to subject business to Constitutional scrutiny). Perhaps recognizing that no explicitly stated right of privacy exists in the Constitution, Warren and Brandeis resorted to the common law to find relief for perceived invasions of privacy.

9. Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1345 (1992).

10. Warren & Brandeis, *supra* note 1, at 195 (*quoting* Cooley on Torts, 2d ed. at 29).

It was the mid-to-late 1800s. The Civil War had ended a few years earlier, and America was in the process transforming and advancing technologically, especially in the press. In the 1870s, faster presses and linotypes became available that provided higher quality text and photographs and printed at speeds as high as 24,000 twenty-four-page newspapers per hour.[11] Over the next twenty years, that speed would nearly triple to 60,000 newspapers per hour.[12] Newspapers also used monster typefaces[13] and color to attract attention, and journalists used typewriters and fountain pens[14] to make news reporting and article writing faster. The concept of the pre-Civil War era penny press was revitalized nationwide due to these advances, and the sensational reporting[15] that came with them ignited the massive popularity of the newspaper.[16] The press was reporting "the curious, dramatic and unusual, providing readers 'a palliative of sin, sex, and violence.'"[17] The attraction of such sensational reporting was noteworthy and caused remarkable growth in the newspaper industry. Even the Boston *Globe* "focused on sensationalism, big headlines, and features . . . ."[18] In the twenty years before Warren and Brandeis published their article, the number of newspapers in the United States increased from roughly 3500 to over 12,000.[19]

Arthur M. Schlesinger, Sr. asserts, "Undoubtedly, [sensational journalism was robbing] American life of much of its privacy to the gain chiefly of morbid curiosity."[20] The press had, without question, exceeded the bounds of then considered standards of decorum,[21] where proper Bostonians regarded the appearance of their names in newsprint as a disgrace.[22] Yet, journalists of that time engaged in "keyhole journalism"[23] and believed that "everything and

---

11. GEORGE H. DOUGLAS, THE GOLDEN AGE OF THE NEWSPAPER 84-86 (Greenwood Press 1999).

12. *Id.* at 84.

13. *Id.* at 114.

14. ARTHUR M. SCHLESINGER, SR., THE RISE OF THE CITY 191 (Macmillan Co. 1933).

15. The New York *World* gained notoriety for headlines like "BAPTIZED IN BLOOD," and, after several hundred children died during a particularly horrible heat wave, "HOW BABIES ARE BAKED." JOYCE MILTON, THE YELLOW KIDS xi-xii (Harper & Row 1989).

16. *See* Gormley, *supra* note 9, at 1350 n.75.

17. *Id.* at 1351 n. 76 (*quoting* EDWIN EMERY & MICHAEL C. EMERY, THE PRESS AND AMERICA: AN INTERPRETIVE HISTORY OF THE MASS MEDIA 349-50 (3d ed. 1972)). *See also* TED GOTTFRIED, THE AMERICAN MEDIA 38 (Franklin Watts 1997). "The Sun didn't follow national and international events in a factual and detached way . . . . [It gave] the people what they wanted: stores of crime and heroism, sacrifice and accidents, misfortune and violence, and, eventually, sex . . . ." *Id.* Such reporting became colloquially known as "yellow journalism" for its use of lurid features and sensational news stories to attract readers and increase circulation.

18. DOUGLAS, *supra* note 11, at 106.

19. *See* FRANK L. MOTT, AMERICAN JOURNALISM 411 (Rev. ed., McMillan Co. 1953).

20. SCHLESINGER, *supra* note 14, at 194.

21. Elbridge L. Adams, *The Right of Privacy, and Its Relation to the Law of Libel*, 39 AM. L. REV. 37, 50 (1905). One notable exception was Whitelaw Reid, editor of the New York *Tribune*. "He ran a very solid, genteel, and dull newspaper: a bulwark against the sensationalism and the vulgarities of yellow journalism of the 1890s." DOUGLAS, *supra* note 11, at 88.

22. TOM GOLDSTEIN, KILLING THE MESSENGER: 100 YEARS OF MEDIA CRITICISM 5 (Columbia University Press 1989).

23. MOTT, *supra* note 19, at 444. Mott notes:

> Closely connected with sensationalism as a major object of attack by the many critics of the press was the invasion of privacy by prying reporters. The prevalence of gossip and scandal stories, in which innocent persons were frequently dragged into the columns of newspapers . . . was no less than indecent; yet it was a part of the formula upon which the great circulations of the period were based.

everyone was everyone's business.'"[24] Warren and Brandeis themselves believed that the media's use of technological advances invaded privacy to no small degree: "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[25] History provides little doubt that this significant loss of privacy that accompanied the transformation in the press, both in technological advances and abusive journalistic style, was the catalyst that drove Warren and Brandeis toward writing *The Right to Privacy*.[26]

Technology and Privacy

Since the days of Warren and Brandeis, technology has continued to advance and to be used to invade privacy. The Internet,[27] one of the wonders of modern technology,[28] has arguably become a utility – a necessity of daily life in America and much of the industrialized world. The terms-of-art of the Internet can commonly be heard from random people on the street.[29] Students can now research an almost infinite number of topics.[30] Family members can communicate in real-time, both with their voice and through typewritten chats, from anywhere on the globe.[31] Corporations advertise their products and services on the worldwide web and enable consumers to purchase a wide variety of goods and services without ever leaving their homes. The Internet has become one of the chief communications tools for employers as well. It allows virtually instantaneous transmission of documents, electronic mail, and other data to consumers, creditors, business partners, and subsidiaries worldwide.

Id.

24. GOLDSTEIN, *supra* note 22, at 5.

25. Warren & Brandeis, *supra* note 1, at 195.

26. Gormley, *supra* note 9 at 1352. The story behind the events that caused Warren to become upset with the media varies storyteller to storyteller. One tale tells of a photographer who snapped perambulatory pictures of Warren's baby girl, thus infuriating Warren by the photographer's invasion of her privacy. *Id.* at 1349. Another tells of Warren's dislike of the Boston papers' treatment of his wife's elite social functions, reporting on them in "highly personal and embarrassing detail." William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960). According to Prosser, the matter "came to a head" when the newspapers "had a field day" when Warren's daughter was married. *Id.* Gormley discounts the wedding story, as Warren's daughter was only six years old when the privacy article was published. Gormley, *supra* note 9 at 1349. "Thus, the old wives' tale (or 'young lady's tale') that has generally been circulated to explain the privacy article appears as fatuous as the newspaper gossip which Warren and Brandeis chided." *Id.*

27. What is now known as the Internet was originally named the ARPANET. *See* Barry M. Leiner et al., *A Brief History of the Internet*, Aug. 4, 2000, *at* http://www.isoc.org/internet/history/brief.html (on file with the author). "The original ARPANET grew into the Internet." *Id.* For simplicity, I refer to both the ARPANET and the Internet as the Internet.

28. *See* ACLU v. Reno, 929 F. Supp. 824, 831 (E.D. Penn. 1996) (discussing development of the Internet). *See also* Leiner, *supra* note 27 (providing brief history of the development of what is now known as the Internet).

29. Leiner, *supra* note 27.

30. *ACLU*, 929 F. Supp. at 842. "It is no exaggeration to conclude that the content on the Internet is as diverse as human thought." *Id.*

31. *Id.* at 835 (describing forms of real-time interpersonal communication on the Internet).

From its inception, the Internet was described as a way of providing social interaction.[32] While the Internet was originally designed to allow remote users to access powerful centrally located supercomputers,[33] human interactivity soon dominated. Three years after the Internet's creation, the first "hot" network application was introduced: electronic mail.[34] E-mail quickly became the most used network application and an omen for the expansive use of networking for "people-to-people" traffic.[35] From the first message, e-mail became, and continues to be, one of the most popular services available on the Internet. E-mail is a dominant form of communication in the workplace, with an estimated 2.8 billion messages sent in the year 2000 alone.[36]

TECHNOLOGY AND MONITORING

Negative Consequences of E-mail Use

E-mail has exposed employers to a multitude of unexpected problems ranging from sexual harassment liability[37] to economic espionage.[38] As e-mail is an efficient medium for distributing data, "it is a common practice to forward off-color jokes or other objectionable materials to multiple recipients."[39] As such, "[e]-mail is a perfect vehicle for harassment."[40] Employers are concerned with being subject to civil or criminal liability for creating, or allowing to be created, a hostile work environment when its employees send offensive e-mail messages.[41] Employers may also be liable under the Civil Rights Act of 1964 and comparable state anti-discrimination laws.[42] For example, in 1995 – early in the development of sexual harassment law – Chevron Corp. agreed to pay $2.2 million to settle sexual harassment charges lodged against it based on, among other things, an e-mail that had circulated about "25 Reasons Why Beer is Better than Women."[43] There have been several notable instances where employer monitoring of e-mail has resulted in the firing or disciplining of the monitored employees.[44] First Union fired seven employees for sending

32. Leiner, *supra* note 27. "In a few years, men will be able to communicate more efficiently through a machine than face to face." J. C. R. Licklider & Robert W. Taylor, "The Computer as a Communication Device," *Science and Technology*, April 1968, *available at* http://memex.org/licklider.pdf (on file with author).

33. *See* ACLU v. Reno, 929 F. Supp. 824, 831 (E.D. Penn. 1996) (asserting original intent of ARPANET to communicate between machine and humans).

34. Leiner, *supra* note 27.

35. *Id.*

36. *See Electronic Privacy: Hearing on H.R. 4908 Before the Subcomm. on the Constitution, Comm. on the Judiciary*, 106th Cong. 2000 WL 1268420 (2000) (statement of Kenneth C. Segarnick, Esquire) (discussing forms of electronic employee monitoring).

37. *See generally* Tony Keller, *The Spying Game: Why sexual harassment law means your boss has to spy on you*, National Post National Magazine, January 1, 2001, at 13.

38. *See* Segarnick, *supra* note 36.

39. MICHAEL RUSTAD & CYRUS DAFTARY, E-BUSINESS LEGAL HANDBOOK § 9.02[D] (Aspen Law & Business 2001).

40. Emily Madoff, *E-Mail's Role in Hostile Work Environment*, New York Law Journal, Aug. 23, 1999, at S6.

41. *See* RUSTAD & DAFTARY, *supra* note 39, at § 9.02[D].

42. *Id.*

43. *See* Madoff, *supra* note 40.

44. *See* Privacy Foundation, *Workplace Surveillance is the Top Privacy Story of 2000*, PR Newswire,

pornographic or otherwise inappropriate e-mail, which included sexually explicit videos.[45] Brokerage-house Edward D. Jones & Co. disciplined 41 people and fired 19 others after one employee filed a complaint based on an e-mail that had circulated through the company headquarters.[46] Solomon Smith Barney fired two high-level analysts after they allegedly transmitted offensive material in violation of the firm's policy.[47] Employers clearly are taking e-mail abuses seriously and are using automated means to discover and prevent these problems.

Monitoring Types

In an effort to counter these kinds of problems, employers are engaged in a "corporate crackdown" on improper use of the Internet and e-mail by using automated monitoring systems.[48] Automated employee monitoring software systems have become very sophisticated. These systems "can record, filter, and sort every word of every e-mail that employees type."[49] There are systems specifically designed to scan for key words and phrases at a rate of 50,000 e-mail messages per hour.[50] Even software that has a core purpose other than to monitor e-mail, such as anti-virus and spam blocking software, can be used creatively to monitor.[51] Other systems can be as obtrusive as to record every single keystroke on the employee's computer.[52] Applications such as pcAnywhere allow remote computer system administrators to view the computer screens of remote computer users in real-time, and can be used to monitor unsuspecting employees' computer activities.[53] Monitoring comes in many forms and can be done without an employee's knowledge or detection.[54]

Dec. 28, 2000. "'Employees are toast,' one chief privacy officer [said], noting that employers have substantial economic, legal—and now, technical—clout over employees in this area." *Id*.

45. Pamela L. Moore, *First Union Fires 7 for sending 'inappropriate' e-mail*, The Charlotte Observer, Aug. 26, 1999, at 1A.

46. *Id*.

47. Pradnya Joshi, *Net Firings on Wall Street*, Newsday (New York), April 1, 1998, at A55.

48. *See* Segarnick, *supra* note 36 (providing examples of "corporate crackdown"); s*ee also* Allison R. Michael & Scott M. Lidman, *Monitoring of Employees Still Growing—Employers Seek Greater Productivity and Avoidance of Harassment Liability; Most Workers Have Lost on Privacy Claims*, The National Law Journal, Vol. 23, No. 23, January 29, 2001, at B9 (same).

49. *See Electronic Privacy: Hearing on H.R. 4908 Before the Subcomm. on the Constitution, Comm. on the Judiciary*, 106th Cong. 2000 WL 1257244 (2000) (statement of James X. Dempsey, Senior Staff Counsel, Center for Democracy and Technology) (discussing various types of e-mail monitoring software).

50. *Id.* It is unclear if such systems could be engineered to distinguish between e-mail sent or received by employees and those by the employer.

51. *See* Segarnick, *supra* note 36. Segarnick alludes that any software that analyzes Internet traffic could be used to monitor employees. For example, anti-virus software routinely scans all e-mail in an effort to catch infected e-mail before it is delivered to the e-mail recipient. Anti-virus software can log to whom the e-mail was sent and who sent it along with other information relevant to the software's core purpose.

52. *Id.* (discussing forms of electronic employee monitoring).

53. *See generally* Symantec Corp., "pcAnywhere", *at* http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=2l (last visited April 16, 2001) (on file with author). Applications like pcAnywhere not only allow system administrators to view the contents of computer screens, administrators can actually take control of the computer and open and view any document, including e-mail, directly from the employer's computer without the knowledge of the employee. *See* Symantec Corp., "Symantec pcAnywhere 10.0 Product Specifications," *at* http://enterprisesecurity. symantec.com/PDF/pca10_fs.pdf (last visited April 16, 2001) (on file with author).

54. *See* Segarnick, *supra* note 36.

Often such systems are installed without any notification to employees that their e-mail is being monitored.[55]

Many employers utilize monitoring systems. An estimated two-thirds of U.S. businesses monitor their employees in one form or another.[56] Statistics as of September 2000 show that about 17% of the Fortune 1000 companies use software to monitor their employee's overall computer activity, and was expected to grow to 80% by 2001.[57] As early as 1993, a survey revealed, of those companies that monitor employees, 73.8% search computer files, 41.5% examine employee e-mail, while only 15.4% review voicemail.[58] Of those that monitor e-mail, 16% do not notify their employees of the monitoring activity.[59] It is clear that the technology to secretly monitor employees exists and is being used by employers.

Effect of Monitoring on Employees

Employers have the ability to examine every aspect of an employee's activities at work.[60] Labor organizations dislike employee monitoring and assert that "concealed surveillance combines the worst features of 19th-century factory labor relations with 20th-century technology, creating an electronic sweatshop."[61] While the threats of liability for allowing a hostile work environment and of economic espionage give employers compelling reasons to monitor their employees' electronic communications, such monitoring is not without consequence.

Physical and Mental Effects

Monitoring of employees has a negative effect on the physical and mental well being of employees. A two-year University of Wisconsin study published in 1990 found higher incidents of physical ailments among workers subjected to workplace monitoring, such as backaches and wrist pains, as well as greater degree of fatigue.[62] These same workers also suffered a 15% increase in extreme anxiety and a 12% increase in depression.[63] A study by the National Institute for Occupational Safety and Health mirrored these same findings, and further noted that monitored workers "exhibited a greater degree of stress, depression, anxiety, instability, fatigue and anger."[64] The impact of these

55. Dempsey, *supra* note 49.

56. Liz Stevens, *Employer snooping is legal, and there's not much you can do about it*, Fort Worth Star-Telegram, Sep. 22, 1999.

57. Segarnick, *supra* note 36.

58. Julie A. Flanagan, *Restricting Electronic Monitoring in the Private Workplace*, 43 DUKE L. J. 1256, 1257 n.3 (1994).

59. Segarnick, *supra* note 36. Legislation has been introduced in the House of Representatives to require employee notification of workplace e-mail monitoring by employers. *See generally* Notice of Electronic Monitoring Act, H.R. 4908, 106th Cong. (2000).

60. Flanagan, *supra* note 58, at 1257.

61. *Id.* (*quoting* Communications Workers Of Am., *Legis. Fact Sheet No. 101-2-2, Secret Monitoring* 1-2 (1990)).

62. *Id.* at 1263.

63. *Id.*

64. *Id.* (*quoting* Occupational Health and Safety Letter, *Electronic Monitoring Blamed for Increased*

problems extend beyond the individuals who suffer them, and, by an Office of Technology Assessment estimate, may cost employers up to $75 billion annually in absenteeism, medical expenses, and lost productivity.[65] Employees question the fairness of the use of monitoring, cite an overall negative work environment, and may believe that monitoring indicates that the employee is unproductive and untrustworthy.[66] Such monitoring also may cause a more adversarial relationship between employees and employers.[67]

Erosion of Privacy

While spying on employees has a long history,[68] Americans more than ever feel that advances in technology erode individual privacy. Respondents to a recent poll conducted by the Center for Survey Research and Analysis at the University of Connecticut were as concerned about privacy as they were about other hot issues, such as Social Security.[69] Even President George W. Bush decided to limit the ability of the public to access his private communications by refusing to use e-mail in the White House.[70] The Federal Bureau of Investigation's "Carnivore"[71] e-mail monitoring system also has come under fire, with forty-five percent of the respondents in poll conducted by Pew Internet and American Life Project stating that Carnivore is a threat to the privacy of ordinary citizens.[72] Sixty-two percent of the respondents in the Pew poll want new laws to protect their privacy.[73] Respondents to the Center for Survey Research and Analysis poll want laws that protect their privacy, even if the effect of those laws restrict the free press.[74] The courts and legislatures have responded differently.

Workplace Stress (June 12, 1991).

65. Flanagan, *supra* note 58, at 1263-64.

66. *Id.* at 1264.

67. Stevens, *supra* note 56.

68. *Id.* "Spying on employees goes back to Henry Ford at the turn of the century. The automobile magnate employed 'a bunch of goons' . . . who tracked the off-hours behaviors of Ford's assembly-line workers. Drunkenness and adultery were grounds for firing." *Id.*

69. The Associated Press, *Americans fear erosion of privacy, poll shows*, April 6, 2001, *at* http://www.cnn.com/ 2001/LAW/04/06/privacy.poll/ (on file with author).

70. CNN.com, *Bush gives up e-mail to protect his privacy*, April 5, 2001, *at* http://www.cnn.com/2001/ ALLPOLITICS/04/05/bush.e.mail/ (on file with author). "I used to be an avid e-mailer . . . . I don't want those e-mails to be in the public domain, so I don't e-mail anymore, out of concern for Freedom of Information laws, but also concern for my privacy." *Id.*

71. Carnivore's "beastly moniker" was recently changed to DCS1000 (Digital Collection System 1000). *See* Erich Luening, *Don't be fooled: DCS1000 is still a 'Carnivore' at heart*, Feb. 9, 2001, *at* http://www.zdnet.com/ zdnn/stories/news/0,4586,2684186,00.html (on file with author).

72. The Associated Press, *Americans cite child porn as top Internet danger*, April 3, 2001, *at* http://www.cnn.com/2001/TECH/internet/04/03/internet.concerns.ap/ (on file with author). While Carnivore may be considered a threat, recently released documents from the FBI suggest that it is being used sparingly. In the ten months between October 1999 and August 2000, the FBI used Carnivore 13 times, and a similar system, Etherpeek, 11 times. While the exact number was not disclosed, however, requests for Internet wiretaps have increased by 1850 percent between 1997 and 1999. The Associated Press, *Records show extensive FBI eavesdropping on the Web*, May 4, 2001, *at* http://www.cnn.com/2001/LAW/05/04/ fbi.eavesdropping.ap/ (on file with author).

73. *Id.*

74. The Associated Press, *Americans fear erosion of privacy, poll shows*, April 6, 2001 *at* http://www.cnn.com/2001/LAW/04/06/privacy.poll/ (on file with author).

CURRENT LAW

The Current State of the Law

Employees possess a degree of privacy in the workplace. Some states have codified the privacy right[75] or provided for the right in their state constitution.[76] The courts have, in varying degrees, found that privacy does exist in the private workplace. In order to prevail, the plaintiff must prove that he or she had a reasonable expectation of privacy in the space or materials that were invaded.[77] There is little question regarding the privacy, or lack thereof, of a personal employee's e-mail communications sent, received, and stored at the workplace. Employees in the public sector enjoy a degree of privacy, granted to them by way of the Fourth and Fourteenth Amendments' protections against unreasonable searches and seizures.[78] The United States Supreme Court announced in *O'Connor v. Ortega*[79] that public employees enjoy a degree of privacy that is tempered by variations in each employment relationship, and the degree of privacy that each particular environment can afford is evaluated on a case-by-case basis.[80] Private employees are protected by the Electronic Communications Privacy Act (ECPA), which authorizes criminal sanctions for those who intentionally access e-mail services without or in excess of authorization.[81] Employers, however, may access their own private e-mail

75. *See, e.g.*, MASS. GEN. LAWS ch. 214, § 1B (1998). "[A] person shall have a right against unreasonable, substantial, or serious interference with his privacy." *Id.; see also* Restuccia v. Burk Tech., Inc., No. CA 952125, 1996 WL 1329386, at *3 (Mass. Super. Ct. Aug. 13, 1996) (applying Massachusetts statute to whether private employees had reasonable expectation of privacy in e-mail messages).

76. Only California has extended a constitutional right of privacy to apply against both public and private employers. *See* CAL. CONST. art. 1, § 1; Porten v. Univ. of San Francisco, 134 Cal. Rptr. 839, 842 (Cal. Ct. App. 1976) (finding state constitutional right of privacy for public and private employees); Flanagan, *supra* note 58, at 1265.

77. *See, e.g.*, United States v. Simons, 206 F.3d 392 (4th Cir. 2000) (holding employee lacked legitimate expectation of privacy in light of employer's Internet policy); United States v. Monroe, 52 M.J. 326 (C.A.A.F. 2000) (finding no reasonable expectation of privacy where employee consented to monitoring when accessing computer system); K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632 (Tex. App. 1984) (finding expectation of privacy when employee provided own lock to secure employer owned locker).

78. *See* U.S. CONST. amends. IV and XIV; O'Connor v. Ortega, 480 U.S. 709 (1987) (discussing context in which public employees have reasonable expectation of privacy in the workplace). "The employee's expectation of privacy must be assessed in the context of the employment relation . . . . Given the great variety of work environments in the public sector, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis." *Id.* at 717-18. *But see* Star Publ'g Co. v. Pima County Attorney's Office, 891 P.2d 899 (Ariz. 1995) (finding public documents are presumed open to public without contrary demonstration furthering a public or private interest). "[W]e doubt that public employees have any legitimate expectation of privacy in personal documents that they have chosen to lodge in public computer files . . . ." *Id.* at 901.

79. O'Connor v. Ortega, 480 U.S. 709 (1987).

80. *Id.* at 717-18.

81. Electronic Communications Privacy Act, 18 U.S.C. § 2701(a) (1994).

> Except as provided in subsection (c) of this section whoever (1) intentionally accesses *without authorization* a facility through which an electronic communication service is provided; or (2) intentionally *exceeds an authorization* to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished . . . .

Id. (emphasis added).

system with full authority.[82] Thus, employees have no cause of action against employer monitoring under the ECPA. Recognizing this, employees have turned to tort law to find legal protection.

The Tort: Intrusion Upon Seclusion

The common law already recognizes the tort of intrusion upon seclusion, based on Warren and Brandeis' article. Warren and Brandeis envisioned the right of privacy as empowering individuals to control to what extent their thoughts would be communicated to others.[83] It did not matter in what form the expression was made, nor the degree of the quality of the expression.[84] The right would only be lost when its creator made the information publicly available.[85] A violation of that privacy would be actionable at law. The common law tort echoes Warren and Brandeis' beliefs.

The Restatement (Second) of Torts defines the invasion of the right of privacy as an "unreasonable intrusion upon the seclusion of another."[86] Intrusion upon seclusion is further defined as occurring by "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offensive to the reasonable person."[87] The comments to § 652B of the Restatement make it clear that such intrusion may be actual physical intrusion, such as entering the home of another over his objection.[88] The intrusion may also, for example, occur by examination of private and personal postal mail.[89] The comments also make clear that public information, either by operation of law or by one's own appearance in public, cannot be considered private, thus any alleged intrusion would not be into one's privacy.[90] The invasion must also be "highly offensive to the ordinary man, as the result of conduct to which the reasonable man would strongly object."[91] Unlike other torts, in Warren and Brandeis' vision, a plaintiff can recover for injury to his or her personality, not simply for actual physical injuries.[92] The plaintiff need not prove monetary damages running from the harm, nor is truth a defense.[93]

82. *See* Wesley Coll. v. Pitts, 974 F. Supp. 375 (D. Del. 1997) (discussing interplay between Title I and II of ECPA).

83. *See* Warren & Brandeis, *supra* note 1, at 198.

84. *Id.* at 198-99. "The same protection is accorded to a casual letter or an entry in a diary and to the most valuable poem or essay, to a botch or daub and to a masterpiece." *Id.* at 199.

85. *Id.* at 199.

86. RESTATEMENT (SECOND) OF TORTS § 652A(2)(a) (1976).

87. *Id.* at § 652B.

88. *Id.* at § 652B cmt. b.

89. *Id. See also* Vernars v. Young, 539 F.2d 966, 969 (3d Cir. 1976) (recognizing cause of action for violation of expectation of privacy in postal mail by employers).

90. RESTATEMENT (SECOND) OF TORTS § 652B cmt. c. (1976).

91. *Id.* at cmt. d.

92. Gormley, *supra* note 9, at 1346.

93. *Id.* at 1345. It is clear that the truth of the matter is of no relevance, as the privacy tort aims to protect the secrecy of the information, which is likely to be true in the first instance. To allow truth to be a defense for an invasion of privacy would allow exactly that which we are trying to protect against, the acquisition of personal and private information, to be a defense against the wrongful act itself.

Smyth v. Pillsbury Co. and McLaren v. Microsoft Corp.

While employees would seem to have a right of privacy protected by the intrusion upon seclusion tort, private employees nonetheless enjoy virtually no privacy in their e-mail, and have little reasonable expectation of it.[94] Two recent cases support this notion: *McLaren v. Microsoft Corp*.[95] and *Smyth v. Pillsbury Co.*[96] In *McLaren*, the plaintiff was terminated from Microsoft's employ after it discovered incriminating information on Microsoft's e-mail system during an investigation into accusations of sexual harassment and theft.[97] The information was in an e-mail folder that was used by McLaren and had been password protected by him.[98] McLaren sued, claiming an invasion of privacy by Microsoft.[99] He asserted that Microsoft recognized McLaren's manifestation of an expectation of privacy by allowing McLaren to password protect the personal folder.[100] The court denied McLaren's claim, stating, "the e-mail messages contained on the company computer were not McLaren's personal property, but were merely an inherent part of the office environment."[101] It further found that McLaren's e-mail was "first transmitted over the network and were at some point accessible by a third-party. Given these circumstances, we cannot conclude that McLaren, even by creating a personal password, manifested—and Microsoft recognized—a reasonable expectation of privacy in the contents of the e-mail messages . . . ."[102]

In *Smyth*, the plaintiff sued under the tort of invasion of privacy after he was fired for sending inappropriate and unprofessional comments through the Pillsbury e-mail system.[103] Pillsbury had repeatedly assured the plaintiff that all e-mail communications would remain confidential and would not be used as grounds for termination or reprimand.[104] The Eastern District of Pennsylvania denied Smyth's claim, stating that there is no "reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management."[105] Notably, the conclusion in *Smyth* is further supported when the employer has issued an acceptable Internet use policy or provides other notice to its

94. *See* Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (finding company's interest in preventing inappropriate e-mail activity on its systems outweighs any employee privacy interest); McLaren v. Microsoft Corp., No. 05-97-00824-CV, slip op. at 5 (Tex. App. May 28, 1999) (finding no expectation of privacy despite password protecting e-mail folder). *See also* Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Informational Practices*, 2000 WIS. L. REV. 743 (2000). "Most participants in the American workplace leave their informational privacy at the door of work." *Id.* at 770; Larry Armstrong, *Someone to Watch Over You*, Bus. Wk., July 10, 2000. "When it comes to privacy in the workplace, you don't have any." *Id.* at 189.

95. McLaren v. Microsoft Corp., No. 05-97-00824-CV, slip. op. (Tex. App. May 28, 1999).

96. Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996).

97. McLaren v. Microsoft Corp., No. 05-97-00824-CV, slip op. at 1 (Tex. App. May 28, 1999).

98. *Id.*

99. *Id.*

100. *Id.* McLaren admitted, however, that it was possible for Microsoft to decrypt the password. *Id.*

101. *Id.* at 4.

102. McLaren v. Microsoft Corp., No. 05-97-00824-CV, slip op. at 4 (Tex. App. May 28, 1999).

103. Smyth v. Pillsbury Co., 914 F. Supp. 97, 98 (E.D. Pa. 1996).

104. *Id.*

105. *Id.* at 101.

employees indicating that electronic communications are subject to monitoring by the employer.[106]

One court has commented on the applicability of the tort of intrusion upon seclusion to an employer reading the personal postal mail of an employee. In *Vernars v. Young*,[107] the Court of Appeals for the Third Circuit opined that where a corporate officer had, without authority, opened and read mail that had been addressed and delivered to Vernars at the corporate offices, but marked personal, would constitute an intrusion upon seclusion.[108] This case suggests that a common law right of privacy may exist in one's personal mail, and further that the expectation of privacy in one's personal mail would be reasonable, even in the workplace.[109] If so, it can also be inferred, since the unauthorized reading of postal mail was considered actionable activity, such activity invades privacy and is also "highly offensive to a reasonable man."[110] The courts have not extended this line of thinking to cover e-mail despite the similarities between e-mail and postal mail.

While one court has extended the reach of *O'Connor v. Ortega* to cover employee privacy in the private workplace,[111] it is apparent that the courts generally are not willing to extend the right of privacy to include e-mail that is sent and received in the private workplace. The *McLaren* decision stands for the proposition that e-mail, if transmitted in a fashion that a third-party may intercept and read the messages, carries with it no expectation of privacy. This is true even if the messages are subsequently hidden in password-protected folders. The *Smyth* decision stands for the idea that employers may monitor e-mail, regardless of any assurances that such monitoring would not occur, even if those assurances would implicitly manifest an expectation of privacy in the employee. The result in *Smyth* has been noted in congressional testimony and used to support efforts to curtail an employer's ability to monitor.[112]

POSSIBLE SOLUTIONS TO PROTECT PRIVACY

Legislative Efforts to Protect Employee Privacy

Monitoring has caught the attention of members of Congress, who recognize the need to notify employees of monitoring activities by their employer.

106. *See* United States v. Monroe, 52 M.J. 326 (C.A.A.F. 2000) (finding no reasonable expectation of privacy where employee consented to monitoring when accessing computer system); United States v. Simons, 206 F.3d 392 (4th Cir. 2000) (holding employee lacked legitimate expectation of privacy in light of employer's Internet policy). *But see* RUSTAD & DAFTARY, *supra* note 39 at § 9.04[D] (noting failure to enforce an Internet usage policy creates an estoppel argument).

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

108. *Id.* at 969. "Just as private individuals have a right to expect that their telephonic communications will not be monitored, they also have a reasonable expectation that their personal mail will not be opened and read by unauthorized persons." *Id.*

109. *See* Laurie Thomas Lee, *Watch your E-Mail! Employee E-Mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop"*, 28 J. MARSHALL L. REV. 139, 166 (1994)

110. *See supra* notes 86-93 and accompanying text (detailing elements for tort of intrusion upon seclusion).

111. *See* Dir. of the Office of Thrift Supervision v. Earnst & Young, 795 F. Supp. 7, 10 (D.D.C. 1992) (applying *O'Connor* to question of employee privacy in diaries containing personal and company data).

112. *See* Segarnick, *supra* note 36 (using *Smyth* case to illustrate employer monitoring practices).

Legislation has been introduced in Congress that would require employers to notify employees of any monitoring of computer usage or electronic communications.[113] The Notice of Electronic Monitoring Act (NEMA)[114] was introduced to bring uniformity to inconsistent workplace e-mail privacy rules.[115] The Act requires clear and conspicuous employee notification of monitoring activities of any electronic type, and that notification is provided annually and whenever monitoring policies change.[116] The notice must include the form of monitored communications, the manner in which the monitoring is accomplished, the frequency of monitoring, the type of information obtained through monitoring, and how such information is stored, used, and disclosed.[117] NEMA caps monetary damage awards at $20,000 per employee and $500,000 aggregate of all damage awards for a given violation.[118]

Disclosure by an employer of its e-mail monitoring practices creates at least two positive effects. First, an employee is put on notice that monitoring may occur. If the employee does not agree with the monitoring practices, the employee may search for alternative employment. Secondly, there will be no ambiguity as to whether there will be monitoring. As such, the employee is put on notice that any e-mail may be read by others. This will provide a sense of clarity over what the employer's expectations are of the employee. If an employee knows that the employer could read any e-mail written or received at work, the employee is less likely to engage in activity that could subject the employee to reprimand or termination.

In some jurisdictions, current law may also protect employers from monitoring in violation of NEMA. The NEMA requirement of notification of monitoring practices would make such notifications akin to corporate policy. Reliance by employees on such a corporate policy to protect their privacy will be met with mixed results. In Massachusetts, for example, provisions in a personnel manual may be enforceable as an express contract against the employer.[119] Intrusions into privacy in violation of provisions in an employee handbook would give rise to a breach of contract claim. The existence of such a provision would also infer an employer-recognized expectation of privacy to the extent not covered by the NEMA requirements, paving the way to an

113. At least one state has also considered similar legislation. *See* S.B. 1822, 1999-00 Reg. Sess. (Cal.) (prohibiting "secret monitoring" of employee generated computer records or e-mail). A previous version of this legislation was enacted by the California legislature, but vetoed by Governor Gray Davis. Governor Davis believed that such legislation opened the employer to lawsuits and trampled on existing employer rights. *See* Deborah Kong, *California Governor Vetoes Ban on Secret E-mail Monitoring by Firms*, San Jose Mercury News, Oct. 12, 1999.

114. Notice of Electronic Monitoring Act, H.R. 4908, 106th Cong. (2000).

115. *See* Segarnick, *supra* note 36 (noting courts that have addressed workplace e-mail privacy have developed inconsistent rules).

116. H.R. 4908 § (a)(1)(B).

117. *Id.*

118. H.R. 4908 § (d)(3)(A)-(B).

119. *See* O'Brien v. New England Tel. & Tel. Co., 422 Mass. 686, 691 (1996) ("A personnel manual may form the basis for an express contract [between employer and employee]."); *see also* Richard J. Pratt, *Unilateral Modification of Employment Handbooks: Further Encroachments on the Employment-at-Will Doctrine*, 139 U. PA. L. REV. 197, 208-9 n.76 (1990) (citing cases from 34 jurisdictions where promises made in employee manual may be binding on employer).

intrusion upon seclusion claim.[120] In other states where such a law does not exist, employers may ignore their own policy, at will, with no recourse to the employee beyond the NEMA remedies.[121] Reliance in good faith on the policy may not be sufficient to protect employee privacy. The law should afford additional protections.

In states where employees may not be protected under contract law, the NEMA protections alone are not adequate to protect employee privacy. NEMA's focus is disclosure, not elimination, of monitoring, and the requirement of notice may operate more as a disclaimer of liability as opposed to an actual protection of employee's privacy.[122] It would also diminish employees' expectation of privacy by effectively being put on notice of the monitoring activities.[123] Such a diminishment would make it difficult to proceed against an employer for committing an invasion of privacy tort.[124] While NEMA is supposed to provide a means of protecting employee privacy, the effect seems to be the opposite.

Recognition of a New Tort: Intrusion Upon Electronic Workplace Seclusion

As Warren and Brandeis recognized, "Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual . . . the right 'to be let alone.'"[125] One can only presume that the stress of the modern workplace, aggravated by technological advances, is more onerous than that which Warren and Brandeis complained of when they said, "modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury."[126] Recent studies seem to confirm this premise.[127]

The right of privacy can be defined as protecting the sanctity of our personhood, our individual selves.[128] The common law already provides a remedy for damages against our mental personhood in the torts of intrusion upon seclusion, but it also protects our mental personhood under the theory of negligent infliction of emotional distress (NIED). NIED is a cause of action that arises when an "actor unintentionally causes emotional distress to another," but only when the actor "should have realized that his conduct involved an

120. It seems unlikely that an employer would take on such limitations and voluntarily give up its right to inspect employee e-mail with impunity. This same principle, however, applies where an employee has the bargaining power to negotiate such a provision into an employment contract.

121. *See, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (finding no reasonable expectation of privacy by employee despite assurances by employer to the contrary).

122. *See Electronic Privacy: Hearing on H.R. 4908 Before the Subcomm. on the Constitution, Comm. on the Judiciary*, 106th Cong. 2000 WL 1586129 (2000) (statement of Marc Rotenberg, Executive Director, Electronic Privacy Information Center).

123. *Id.*

124. *See supra* notes 86-93 and accompanying text (discussing current privacy tort law).

125. Warren & Brandeis, *supra* note 1, at 195.

126. *Id.* at 196.

127. *See supra* notes 62-67 and accompanying text (discussing psychological and physical harm caused by monitoring).

128. *See supra* note 6 and accompanying text (providing a definition of privacy).

unreasonable risk of causing the distress," and the actor "should have realized that the distress . . . might result in illness or bodily harm."[129]

Employee monitoring may give rise to a NIED claim. Presumably, employers do not normally inflict actionable emotional distress upon their employees. Thus, any emotional distress would likely be unintentional.[130] As previously discussed, the invasion of privacy by way of employee monitoring causes significant physical and mental harm to the employees.[131] The physical manifestation of the mental distress, which is required by the common law, also supports the manifestation of the mental anguish.[132] To prove NIED, the harm caused by the employer's monitoring must be foreseeable. It is foreseeable that an employer's monitoring of what an employee may consider private and personal would cause mental anguish to the employee.[133]

While the application of NIED to employee monitoring may seem to provide a remedy, it does not because the risk of causing distress must be unreasonable.[134] It is unclear, in this context, what degree of unreasonableness would be necessary. Is occasional monitoring sufficient risk of an employee's claim of constant and persistent emotional distress? Is the fear of monitoring sufficient? Does the monitoring need to be consistent, even routine, for an employee to prevail? Such questions cannot easily be answered, and the courts may easily decide differently in similar cases. A new cause of action in tort could be created and used to address the deficiencies in existing law.

The proposed tort combines the elements of NIED and intrusion upon seclusion. The new cause of action has the following elements:

> One who intentionally intrudes, physically, electronically, or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, and in doing so the actor intentionally or negligently causes emotional distress to another, is subject to liability to the other for the invasion of the other's privacy and for the resulting illness or bodily harm.

This new tort proposes to eliminate the problems of applying either NIED or intrusion into seclusion independently to an alleged intrusion. It maintains the common elements of both torts, but also eliminates the problematic reasonableness element and, in a sense, creates strict liability. This may be shocking, but it need not be so.

Both torts aim to protect against mental anguish, and where there is physical harm, reasonableness should be dispensed with.[135] The new tort requires there

---

129. RESTATEMENT (SECOND) OF TORTS § 313(1) (1986).

130. Normal workplace stress is not sufficient to give rise to a NIED claim. *See* Bishop v. State, 899 P.2d 959 (Wash. App. 1995). "[T]he courts cannot guarantee a stress-free workplace. Therefore, we hold that absent a statutory or public policy mandate, employers do not owe employees a duty to use reasonable care to avoid the inadvertent infliction of emotional distress when responding to workplace disputes." *Id.* at 963.

131. *See supra* notes 62-67 and accompanying text (discussing harm caused by monitoring of employees).

132. See RESTATMENT (SECOND) OF TORTS § 436A (1965); *see, e.g.*, Armstrong v. Paoli Mem'l Hosp., 633 A.2d 605 (Pa. Super. Ct. 1993) (holding loss of continence after hospital erroneously notified plaintiff of serious injury to "spouse" sufficient manifestation of physical harm).

133. In light of various studies published on this very phenomenon, actual foreseeability is heightened. *See supra* notes 60-66 and accompanying text (discussing harm caused by monitoring of employees).

134. *See* RESTATEMENT (SECOND) OF TORTS § 313(1)(a) (1986).

135. This does not, of course, address the eggshell plaintiff. However, one must still take such a plaintiff as you find her. *See* Bartolone v. Jeckovich, 481 N.Y.S.2d 545 (1984) (holding defendant must "take a plaintiff

to be physical manifestation of the harm from the intrusion. Without physical harm there is no liability and therefore the tort guards against liability stemming from minor or inconsequential intrusions. The physical harm caused by the intrusion would still need to be recognizable harm under NIED. The harm cannot be transitory, such as temporary fright, nausea, or rage.[136] The harm, further, cannot be inconsequential nor amount to an insubstantial bodily injury.[137] By requiring a legally recognizable physical injury, the tort avoids opening the floodgates of litigation.[138] The actor must also intentionally intrude into the privacy of another. This borrows from the tort of intrusion upon seclusion and avoids liability for accidental encroachment. By combining these two torts, employees will have a new cause of action protecting their privacy where an invasion would be so onerous as to have a physical harm flowing from it. Minor invasions not causing a physical harm would not be actionable.

Using "Code" to Protect Privacy

The law of the land, however, may not change to protect against workplace privacy violations. Employers will, no doubt, battle fiercely against any attacks on right to read employee e-mail. The courts have already taken the stand that employers can monitor and read e-mail with impunity.[139] Lessig wonders what can be done to protect privacy where structures already exist to deny that privacy[140] – his response: "[L]ook to the code."[141] He is not speaking of legislative action; rather, Lessig believes in the power of cyberspace, of computer code, to regulate.[142] While Lessig asserts that such code would need to be developed to protect privacy,[143] such code already exists in the form of encryption software.[144] The use of encryption technology by employees can ensure that private communications in the workplace remain private. The nature of e-mail is akin to mailing a postcard through the U.S. postal system[145] – its contents are easily read by anyone who comes into contact with

---

as he finds him."). In *Bartolone*, the plaintiff suffered relatively minor injuries in a traffic accident that aggravated a pre-existing paranoid schizophrenic condition, causing an acute psychotic breakdown. *Id*. at 546. The court allowed recovery, stating that the plaintiff can be held liable for aggravating a pre-existing illness. *Id*. at 547.

136. *Armstrong*, 633 A.2d at 609 (describing requisite type of harm to recover under NIED).

137. RESTATMENT (SECOND) OF TORTS § 436A cmt. c (1965).

138. *See id*. at cmt. b. "[An] emotional disturbance which is not so severe and serious as to have physical consequences is normally in the realm of the trivial, and so falls within the maxim that the law does not concern itself with trifles." *Id.*

139. *See supra* notes 94-105 and accompanying text (discussing cases denying privacy right over e-mail in private workplace).

140. LESSIG, *supra* note 4, at 163. Lessig was discussing machine-to-machine negotiated privacy systems. *Id.*

141. *Id.* (arguing cyberspace programming code be developed to protect privacy).

142. *Id.* at 6. "In cyberspace we must understand how code regulates – how the software and hardware that make cyberspace what it is *regulate* cyberspace as it is . . . . *Code is law*." *Id.* (emphasis in original).

143. *Id.* at 163.

144. Lessig admits that the Internet is "becoming encryption-rich." *Id*. at 157. He asserts, however, that encryption is not sufficient to deny the government's legitimate demand for information, as courts can compel the decryption of data. *See id*. Since employers cannot compel the decryption of data, including the government *qua* employer, without the authority and force of government behind them, such a distinction is not relevant to this discussion.

145. *But see* Lunney v. Prodigy Servs. Co., 683 N.Y.S.2d 557, 560 (N.Y. App. Div. 1998) (comparing

that postcard.[146] An electronic envelope, therefore, should be sufficient to protect the contents of e-mail from unwanted disclosure, and further, provide at least a reasonable expectation of privacy over the contents of the e-mail. When using encryption, the e-mail is put into a digital envelope that cannot be opened[147] except by the person who holds the decryption key. In its encrypted state, the contents of the e-mail are scrambled and completely illegible to any third party that may come across the e-mail.[148] Encryption provides the envelope.[149]

The courts and Congress have implicitly created an expectation of privacy in postal mail that society recognizes as reasonable.[150] Congress has mandated that "No letter . . . shall be opened except under authority of a search warrant . . . or pursuant to the authorization of the addressee."[151] One hundred twenty five years ago, the United States Supreme Court declared that letters, sealed and transported by the mail, are "fully guarded from examination and inspection . . . as if they were retained by the parties forwarding them in their own domiciles."[152] The United States Court of Appeals for the Third Circuit has opined that the interception and reading of postal mail by an employer that is marked personal and addressed to an employee would likely rise to the level of an intrusion upon seclusion.[153] An encrypted e-mail is essentially the same as a sealed postal letter. Accordingly, where a use of a sealed paper envelope suffices to manifest the expectation, employees who use encryption have manifested a reasonable expectation of privacy. If an employer succeeds in decrypting the e-mail, the employer violates the employee's privacy and may be liable in tort.

Employers may fear that the use of encryption in such a way will provide employees with a secure means to misappropriate intellectual property and other intangible assets. The encryption would prevent employers from

---

"essential nature" of e-mail to that of the written telegraph messages). The court in *Lunney* asserts that e-mail is essentially the same as a telegraph, but then goes on to describe the differences between a telegraph and a modern day telephone call. A telegraph required direct intervention by employees of the telegraph company while a phone call requires no such intervention. *Id.* at 561 (*quoting* Anderson v. New York Tel., 345 N.Y.S.2d 740, 752 (N.Y. App. Div. 1973)). Today's e-mail, on these terms, is actually more akin to a phone call than a telegraph, as no more intervention by the service provider is required to transmit the e-mail than to make a direct-dialed phone call. Such distinctions, and the legal questions raised by them, are outside the scope of this paper.

146. *See* SIMSON GARFINKEL, PGP: PRETTY GOOD PRIVACY xxiii, 8-9 (Deborah Russell ed., O'Reilly & Associates, Inc. 1995) (describing how e-mail is similar to a postcard).

147. Nothing is absolute, and in fact an unauthorized person can open an encrypted e-mail. The simplest way to crack an encrypted message is to use every key combination possible. This method is very time consuming, however, becasue it would take 10^{13} years to crack a 128-bit key at the rate of one billion computers that could try one billion key combinations per second. GARFINKEL, *supra* note 146, at 40. There are other methods of decrypting a message, such as stealing the encryption/decryption keys or booby-trapping the encryption software. *Id.* at 55.

148. *Id.* at 44-45 (showing effects of encryption and decryption).

149. *Id.* at 10. "Encryption is a way of putting an end to this problem once and for all." *Id.*

150. *See* State v. Phaneuf, 597 A.2d 55, 59 (Me. 1991) (Glassman, J., dissenting) (discussing expectation of privacy in mail at common law and under statute).

151. 39 U.S.C. § 3623(d) (1994) (prohibiting inspection of first class mail except in specific circumstances).

152. *Ex parte* Jackson, 96 U.S. 727, 733 (1877) (discussing Fourth Amendment search and seizure protections as afforded to postal mail).

153. Vernars v. Young, 539 F.2d 966 (3d Cir. 1976); *supra* notes 107-110 and accompanying text (discussing privacy expectation in private postal mail).

accessing employee e-mail communications to investigate possible misappropriation. Invading an employee's privacy is not necessary to protect corporate assets, secrets, or other proprietary information. Employers should not expect that encryption would sound the death knoll of asset protection. Employers may protect themselves with confidentiality agreements, covenants not to compete, common law torts such as conversion and misappropriation, and any remedies arising out of corporate espionage. Using available legal tools, employers can ask courts to compel an employee to decrypt any messages relevant to the dispute. This method ensures the employer's interests are protected without violating the interests of the employee.

CONCLUSION

Employees in the private workforce currently enjoy no privacy in their electronic mail communications. Even though legal doctrines exist that would seem to recognize the right of privacy for employees, the courts have been wary to extend that right very far into the workplace. As such, the private employees have been subjected to monitoring of their e-mail communications in the workplace. Employers believe monitoring of employees e-mail will stem liability for abuses such as corporate espionage and fostering a hostile work environment. Monitoring erodes employee privacy, and creates stress that has a direct negative impact on the emotional and physical health of employees. Employees need to be protected against workplace privacy invasions.

The right of privacy has been championed since 1890 when abuses of technological advances were the catalyst for the first legal commentary on the right. Technology has advanced, and has continued to be abused to invade the privacy of individuals. The law should respond to protect employees from harm proximately caused by monitoring. Legislation requiring notification of employees of any monitoring, the creation of a new tort, and employee use of encryption are solutions that can protect against invasions into employee privacy.

Todd M. Wesche