Mailer Daemon: Unable to Deliver Message
Judicial Confusion in the Domain of E-Mail Monitoring in the Private Workplace

Rebecca Ebert

I. INTRODUCTION

American employees have long been deluded as to the depth of privacy protection in the United States. The common perception is that privacy is a fundamental right.[1] The truth is that the right to be let alone is a modern invention: an 1890 Harvard Law Review article initiated the modern day torts of privacy.[2] The privacy tort of intrusion upon seclusion was often relied upon as a common law basis of protection for wronged private employees in the pre-technological boom era.[3] Despite the growing awareness of the need for privacy protection in this country, close to 78% of employers are practicing intrusive electronic monitoring techniques.[4] Employee privacy protections in the workplace under intrusion upon seclusion are being narrowed by the almost complete rejection of plaintiff claims against private employers for monitoring electronic communications.[5] The rules for private employees and those for public employees have developed independently of one another.[6] Based upon which sector the employee works in, the laws are different, the protections are different and the judicial standards are different. Courts were able to keep this

1. *See* Griswold v. Connecticut, 381 U.S. 479, 486 (1965) (remarking that the right to privacy is "older than the Bill of Rights").

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

3. *See, e.g.*, K-Mart Corp. v. Trotti, 677 S.W.2d 632, 637-38 (1984 Tex. App.).

4. American Management Association, 2000 AMA SURVEY ON WORKPLACE TESTING: MONITORING & SURVEILLANCE, SUMMARY OF KEY FINDINGS (2000) [hereinafter "*AMA*], *available at* http://www.amanet.org/research/pdfs/monitr_surv.pdf (reporting that 78% of major United States firms practice some form of electronic oversight). Further, 73.5% of employers "record and review employee communications and activities on the job, including their phone calls, e-mail, Internet connections and computer files". *Id*. Companies surveyed stated that they engage in surveillance for the purposes of performance reviews, legal compliance, legal liability and to measure productivity: "Net surfing, personal use of office e-mail, and/or dialing up 900 numbers expend time and assets on non-business related activities." *Id.* at 1.

5. Most cases involving employees fired for personal and some inappropriate use of the Internet from work results in a finding that the company did not invade the employee's privacy; that poor notification procedures regarding e-mail monitoring, and the ease of the accessing employee messages did not result in a reasonable expectation of privacy. *See, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996).

6. The common law is suggested and adopted by scholars and the courts alike. Common law is the basis for most civil suits in this country, and is where the privacy protections for private employees reside. Public employees are protected by the common law as well, but public employees also have a plethora of federally constructed protections in the Fourth Amendment and the Electronic Communications Privacy Act, among others. *See* the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-22, 2701-11 (1994); *see also* U.S. CONST. amend. IV.

 ISSN 1536-7983

relatively clear in the past (when electronic communications were harder to monitor), but with the introduction of e-mail, virtually unrestrained e-mail monitoring and the numerous civil cases that have developed from that monitoring, many judges seem to be confused as to which standard to apply.[7] Of the cases reviewed in this paper, no court applied the correct standard by which to find an intrusion upon seclusion in the private workplace.[8] The courts in these cases looked at the invasion under the light of whether or not there existed a reasonable expectation of privacy, the test for the Fourth Amendment, available only for invasions by the state, not invasions by a private employer. [9] The correct test, whether the intrusion is highly offensive to the reasonable person, would possibly render a very different result.[10] Judicial confusion is leaving employees (who have brought suit in civil court under the common law) with virtually no protection against employers who monitor their electronic communications.[11] Courts are decreasing the amount of protection available to American employees because electronic communications are so prevalent and easily scrutinized. Courts are concluding that ease of access should somehow translate into an employee having no reasonable expectation of privacy.[12] Intrusion upon seclusion must be reexamined and possibly re-applied to reflect the impact of Internet access and e-mail use in the workplace.[13]

Part II first reviews the private/public employee privacy protection dichotomy. It then reviews the Federal statutory provision regarding interception of electronic communications and the Fourth Amendment protections for public employees. Part II further explores the history and charts the growth of the common law right to privacy and the tort of intrusion upon seclusion and examines the tort's application across other workplace-related intrusions. It also briefly chronicles the rise of advanced network technology in business, up to current day standards. Part II will show that the Fourth

---

7. *See infra* § III.

8. *See, e.g.*, McLaren v. Microsoft, 1999 Tex. App. LEXIS 4103 at 11 (Tex. App. 1999); Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996); Bourke v. Nissan Motor Corp., No. B068705 (Cal. Ct. App. Filed July 26, 1993) (no published decision).

9. *See McLaren*, 1999 Tex. App. LEXIS 4103 at 1; *Smyth*, 914 F. Supp. at 101; *Bourke*, No. B068705 at 1.

10. "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another of his private affairs or concerns, is subject to liability to the other for invasion of privacy, if the intrusion would be highly offensive to a reasonable person." RESTATEMENT (SECOND) OF TORTS § 652B (1977).

11. *See infra* § III(B).

12. *See, e.g.*, *McLaren*, 1999 Tex. App. LEXIS 4103 at 1.

13. *See* RESTATEMENT (FIRST) OF TORTS § 867 (1939) (initiating a cause of action for "a person who unreasonably and seriously interferes with another's interest in not having his affairs known to others or his likeness exhibited to the public is liable to the other."). Drafted in the 1930s, authors of the original tort of interference with privacy were likely unable to comprehend the impact that technology would have on the future. The Internet in and of itself, but also as a means of research (and spying) must have been difficult to envision. The drafters noted that "[t]his interest appears only in a comparatively highly developed state of society. It has not been recognized until recently, not only because it normally involves nothing more that mental distress, but also because there is not a clear line of demarcation between what should and should not be permitted." RESTATEMENT (FIRST) OF TORTS § 867 cmt. b (1939). Indeed, many famous invasion of privacy cases still revolve around physical invasions such as those surrounding "peeping toms." *See, e.g.*, Harkey v. Abate, 131 Mich. App. 177 (Mich. Ct. App. 1983). The current right to privacy has four subsections, the relevant one being intrusion upon seclusion. *See* RESTATEMENT (SECOND) OF TORTS § 652B (1977). "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another of his private affairs or concerns, is subject to liability to the other for invasion of privacy, if the intrusion would be highly offensive to a reasonable person." RESTATEMENT (SECOND) OF TORTS § 652B (1977).

Amendment legal standard of a reasonable expectation to privacy is being applied to private cases. Part III attempts to analogize e-mail to phones and traditional postal mail to prove that e-mail requires a different level of scrutiny in invasion of privacy cases. Further, Part III considers the high level of judicial confusion involved in decisions on e-mail intrusion upon seclusion cases. Part III takes into consideration the ever-changing workplace and proposes an appropriate common law model by which to adjudicate intrusion cases in the workplace and what the elemental test should reflect. This paper concludes that, in an invasion of privacy context, more protection of e-mail and other types of electronic communication is necessary to advance the level of privacy protection in the private workplace.

II. BACKGROUND

A. The Public/Private Dichotomy

The extent of privacy protection in the workplace afforded to an employee depends upon whether or not they work for the government or in the private sector.[14] State action is required before a citizen can invoke a constitutional right, which operates primarily to protect citizens from the government.[15] The actions of a governmental employer may be defined as "state actions."[16] Private employer actions rarely constitute state action because the behavior of private citizens and corporations is not generally controlled by the Constitution.[17] Because of the private/public distinction, public employees may utilize federal statutory and federal and state constitutional rights, where private employees are essentially afforded only common law protection and only limited state and federal statutory protection.[18]

B. Federal Statutory Protections for Private and Public Employees

The statutory backdrop for protection of electronic communications is set forth in the Electronic Communications Privacy Act of 1986 ("ECPA").[19] The EPCA was an amendment to Title III of the Crime Control and Safe Streets Act of 1968, commonly referred to as the Federal Wiretap Act.[20] The ECPA was

14. S. Elizabeth Wilborn, *Revisiting The Public/Private Distinction: Employee Monitoring in the Workplace*, 32 GA. L. REV. 825, 828 (1998).

15. It is well established that state action is the basis for the distinction between public and private activities. *See, e.g.*, Jackson v. Metro. Edison Co., 419 U.S. 345, 359 (1974) (affirming that "the essential dichotomy set forth in [the Fourteenth] Amendment between deprivation by the State, subject to scrutiny under its provisions, and private conduct, 'however discriminatory or wrongful,' against which the Fourteenth Amendment offers no shield"). The *Civil Rights Cases* are frequently credited with being the origin of the state action requirement. The Civil Rights Cases, 109 U.S. 3 (1883).

16. "The phrase 'state action' is used . . . in its generic sense, to refer to action by any level of government, from local to national." Franz v. United States, 707 F.2d 582, 591 n.33 (D.C. Cir. 1983), *modified*, 712 F.2d 1428 (D.C. Cir. 1983).

17. *Franz*, 707 F.2d at 591 n.33. *See also* Edwin Chemerinsky, *Rethinking State Action*, 80 NW. U. L. REV. 503, 507 (considering plaintiff's difficulty prevailing in suits for private employee violations of privacy).

18. *See* Wilborn, *supra* note 14, at 828.

19. The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-22, 2701-11 (1994).

20. *Id.* The intention of the ECPA was to update the law's scope to encompass new technologies and include the interception of electronic communications and stored electronic communications. *See also* Laurie

enacted to update the protection of citizens' civil liberties to recognize the impact of developing technologies.[21] The EPCA makes illegal the interception of both oral and electronic communications.[22]

The EPCA offers employers three methods of exemption from the employee protection offered by the Act: prior consent, business use, and system provider.[23] The prior consent exemption provides that interception of electronic communication is allowed when one party to the communication has given prior consent.[24] The business use exemption requires that the interception be made in the "ordinary course of business."[25] The system provider exemption is available to employers who provide their own company e-mail system.[26] The ECPA has been proved to provide some protection for public sector employees against employer intrusions, specifically when the monitoring invades into an employee's private life.[27] For the private employee, these exemptions essentially cancel out any possible federal protection for private employees from invasions of privacy by their employers.

In *McVeigh v. Cohen*,[28] America Online ("AOL") provided the United States Navy with subscriber information about Senior Chief Timothy McVeigh (no relation to the Oklahoma bombing defendant), an AOL user.[29] The AOL account was McVeigh's private account.[30] The Navy used the information about McVeigh to fire him under "Don't Ask, Don't Tell" after he had sent an e-mail to a crew member's wife regarding a toy-drive she was running for a children's charity.[31] McVeigh had used the alias name "boysrch" in his e-mail, prompting the woman to look it up in the AOL directory and report it; the information eventually reached the Judge Advocate General's (JAG) office.[32]

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, 151 n.62 (1994).

21. *Id*.

22. The EPCA amended the Federal Wiretap Act's definition of "intercept" to include "the aural or other acquisition of the contents of any wire, electronic or oral communication." 18 U.S.C. § 2510(4). The definition of "intercept" and "intercepted" has been thoroughly debated in litigation. *See* Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457 (5th Cir. 1997) (holding that seizure of unread e-mail did not constitute an interception, and there exists a difference between e-mail in "transfer" and e-mail in "electronic storage"). The Fifth Circuit's interpretation of "interception" leaves a very narrow window in which an e-mail may be intercepted (the virtually non-existent period of time between the 'send' command and point when the message is actually sent or saved to the temporary location during routine routing). *See Steve Jackson Games*, 36 F.3d at 462. The end result is that interception under the EPCA is all but impossible.

23. *See* 18 U.S.C. §§ 2511(2)(d); 2511(2)(a)(i); and 2510(5)(a)(ii) (1986).

24. *See* 18 U.S.C. § 2511(2)(d). Although express consent is always the strongest form of protection for the employer, some courts have held that implied consent will be enough to trigger the exemption. *See, e.g.*, Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983) (holding that consent, express or implied, may be partial).

25. *See* 18 U.S.C. § 2511(2)(a)(i). *See also Watkins*, 704 F.2d at 582-84. In *Watkins*, the court held that business calls always fell into this phrase, while personal calls would not necessarily do the same. *Id.* If the personal calls were made on business equipment, then personal calls could be intercepted in the ordinary course of business to determine their nature (but not their content). *Id*.

26. *See* 18 U.S.C. § 2510(5)(a)(ii) (allowing the provider of communications to intercept and monitor messages without violating the EPCA). This has been found to be a successful way for employers to avoid liability. *See generally* Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996) (holding that an employer's search of an employee's computer messages was not a transgression of the federal wiretap laws).

27. *See* McVeigh v. Cohen, 983 F. Supp. 215 (D.D.C. 1998), *reinstated*, 996 F. Supp. 59 (D.D.C. 1998).

28. McVeigh v. Cohen, 983 F. Supp. 215 (D.D.C. 1998), *reinstated*, 996 F. Supp. 59 (D.D.C. 1998).

29. *McVeigh*, 983 F. Supp. at 217.

30. *Id*.

31. *Id*.

32. *Id*. The information in the user profile accessed by the crew member's wife specified that the

The JAG investigator contacted AOL and, without identifying himself as a representative of the government, requested the subscriber information that identified McVeigh as the holder of the e-mail alias "boysrch."[33] Citing harm to McVeigh and the public interest in privacy, the court issued an injunction permitting McVeigh to remain in active service.[34] *McVeigh* is an important case because it provides a limit to employer monitoring of electronic communications by the Federal government. If this were a case between a private employer and their employee, however, the ECPA would be virtually useless due to the many exemptions provided to private employers.[35] The ECPA was a successful tool for the employee in *McVeigh* in part because of the patently discriminatory and invasive behavior of the Navy officers involved.[36]

Moreover, the ECPA is not always successful against government employers.[37] In *Bohach v. City of Reno*, two police officers tried to stop an investigation into the contents of electronic messages sent between them on the police department's pager system.[38] The *Bohach* court found, because a department computer stored the messages for any period of time, regardless of whether it was temporary, intermediate or incidental to an impending electronic transmission, it was an electronic storage.[39] The court further held that " an 'electronic communication,' by definition, cannot be 'intercepted' when it is in 'electronic storage,' because only 'communications' can be 'intercepted.'"[40] Furthermore, the *Bohach* court found that the police department, as system provider, was free to access stored electronic messages as it pleased because of the service provider exception to the ECPA.[41] The *Bohach* decision is an example of when the ECPA protections fail government employees. More often than not, the ECPA is effective device for public employees to use to redress an employer invasion into their electronic communications.[42] The ECPA is just one of the ways that public sector employees may seek protection and redress from invasions of privacy committed by their employers.[43] Public sector employees may also seek protection under the Fourth Amendment.[44]

---

subscriber using the alias "boysrch" was named Tim, that he lived in Honolulu, worked in the military and identified his marital status as gay. *Id*. The profile also included interests such as "collecting pics of young studs" and "boy watching." *Id*.

33. *Id*.

34. *McVeigh*, 983 F. Supp. at 220. Judge Sporkin held that the officer's likely success on the merits of his claims that the Navy violated the "Don't Ask, Don't Tell, Don't Pursue" policy in obtaining the subscriber information from AOL and that they violated his right to privacy under the ECPA supported the injunction. *Id*.

35. *See* 18 U.S.C. §§ 2511(2)(d), 2511(2)(a)(i), and 2510(5)(a)(ii).

36. See *McVeigh*, 983 F. Supp. at 220. The *McVeigh* court specifically cited harm to the public interest in privacy. *Id*.

37. *See e.g.*, Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996).

38. *Bohach*, 932 F. Supp. at 1233.

39. *Id*. at 1236.

40. *Id*.

41. *Id*.

42. *See e.g.*, Amati v. City of Woodstock, 829 F. Supp. 998 (N.D. Ill. 1993); *McVeigh*, 983 F. Supp. 215.

43. The United States Constitution, as well as the statutes and constitution of the state in which they reside protect public sector employees. *See supra* § II B.

44. U.S. CONST. amend. IV.

C. Fourth Amendment Protections for Public Employees

Like many private employers, the Federal Government has established a goal of providing e-mail access to every federal agency and promotes e-mail as a preferred method of conducting business.[45] Public employees have some redress in the ECPA,[46] but the Fourth Amendment also protects them from unlawful search and seizure.[47]

In order to invoke the Fourth Amendment, an employee must have a "reasonable expectation of privacy" in the subject of the search or seizure to invoke the Constitution's protections.[48] The reasonable expectation of privacy test has two elements: "first that a person [has] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[49] In essence, "[w]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[50]

In public employee e-mail cases, this Fourth Amendment shelter has been accepted as a valid method of privacy protection. In *United States v. Maxwell*,[51] a general court-martial convicted Colonel Maxwell of using his personal computer to receive, transmit and distribute child pornography by way of America Online.[52] The court of appeals held that Maxwell had an objectively reasonable expectation of privacy "in those messages stored in computers which he alone could retrieve through the use of his own assigned password."[53] The *Maxwell* court, however, distinguished between messages left on the AOL servers and those downloaded from the server.[54] The court established that "[i]n the modern age of communications, society must recognize such expectations of privacy as reasonable."[55] In the *Maxwell* view, the electronic nature of e-mail is not a detriment to privacy protection.[56]

Private employees have fewer resources: they usually have only the common law to protect them, and it carries little protection against employer e-mail monitoring.[57]

---

45. *See* GOVERNMENT ELECTRONIC MESSAGING PROGRAM MANAGEMENT OFFICE, RECOMMENDATIONS, *available at* http://www.fed.gov/hptext/e-mailpmo/emtf/EMTF8.html.

46. *See supra* § II B.

47. U.S. CONST. amend. IV.

48. The Supreme Court first enunciated the reasonable expectation of privacy test in *Katz v. United States*, 389 U.S. 347, 361 (1967). In *Katz*, government investigators tapped and recorded phone calls made from a public phone booth. *Id*. at 348. The Court held that "the Fourth Amendment protects people, not places." *Id*. at 351. A state action must predicate any invocation of a constitutional right. *See supra* notes 15-16.

49. *Id*. at 361 (Harlan, J., dissenting).

50. *Id*. at 351.

51. United States v. Maxwell, 42 M.J. 568 (A.F. Ct. Crim. App. 1995).

52. *Maxwell*, 42 M.J. at 573.

53. *Id*. at 576.

54. *Id*. at 576. "[Maxwell] may have forfeited his right to privacy to any e-mail transmissions that were downloaded form the computer by another subscriber or removed by a private individual from the on-line service." *Id*.

55. *Maxwell*, 42 M.J. at 576. However, the court affirmed the conviction on other grounds. *Id*. at 583.

56. *Id*. *But see* United States v. Simons, 206 F.3d 392 (4th Cir. 2000) (holding that a public employee had no reasonable expectation of privacy in files downloaded from the Internet because the employer's Internet policy states that the employer would "audit, inspect and/or monitor employee's use of the Internet, including all file transfers, all websites visited, and all e-mail messages, 'as deemed appropriate.').

57. *See infra* § III.

D. Development of the Common Law Right to Privacy

The common law right to privacy is a relatively recent invention, first widely accepted after the publication of Samuel D. Warren and Louis D. Brandeis' 1890 Harvard Law Review article entitled "The Right to Privacy."[58] The Restatement (Second) of Torts has delimited four torts for invasion of privacy: unreasonable intrusion upon seclusion of another, appropriation of another's name or likeness, unreasonable publicity of another's private life and placing another in a false light in public.[59] The assertion of a common law right to privacy initially met with resistance,[60] but was eventually accepted in most jurisdictions.[61] The tort most commonly used in workplace privacy cases is intrusion upon seclusion.

To prevail on a claim for intrusion upon seclusion, a plaintiff must show that the allegedly tortious intrusion would be highly offensive to a reasonable person.[62] There is no requirement that any information be obtained or communicated to another; rather it is the intrusion itself which constitutes the tort.[63] No trespass need be committed to satisfy the elements of the tort.[64] In the cases in which employees have brought invasion of privacy claims against employers for e-mail monitoring, few have been able to convince the courts that the standard has been met.

---

58. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). The article was reportedly written in response to Warren's distress over newspaper coverage of a family wedding. JOHN L. DIAMOND, LAWRENCE C. LEVINE, M. STUART MADDEN, UNDERSTANDING TORTS 437 (Matthew Bender 1998) (1996). The article centered on the increase of gossip in the newspapers, and the detrimental effect to the solitude and privacy of those reported on. *See* Warren & Brandeis, 4 HARV. L. REV. at 196.

59. *See generally* RESTATEMENT (SECOND) OF TORTS § 652A. Sections 652B-E provide further coverage of these torts.

60. *See* Roberson v. Rochester Folding Box Co., 171 N.Y. 538 (1902) (holding that there was no protection against conduct constituting an invasion of privacy in the New York courts). In *Robertson*, the plaintiff attempted to prevent the Franklin Mills Co. from using her picture (a lithographic print) in advertisements for their flour. *Id*. at 542. The court held that the "so-called right of privacy," had not yet been recognized in New York, and refused to recognize it, as doing so would "[do] violence to settled principles of law by which the profession and the public have long been guided." *Id*. at 556. The *Robertson* court stated that "attempts to logically apply the principle will necessarily result, not only in a vast amount of litigation, but in litigation bordering upon the absurd . . . ." *Id*. at 545. The New York legislature responded to the *Robertson* decision by enacting a statute that made it a misdemeanor to engage in the equivalent of the current day privacy tort of appropriation. *See* 1903 N.Y. Laws 132, §§ 1, 2.

61. *See*, *e.g.*, Pavesich v. New England Life Insurance Co., 122 Ga. 190 (1905).

> Personal liberty includes not only freedom from physical restraint, but also the right 'to be let alone,' to determine one's mode of life, whether is shall be a life of publicity or of privacy, and to order one's life and manage one's affaires that may be most agreeable to him, so long as he does not violate the rights of others or of the public.

Pavesich, 122 Ga. at 192. "By becoming a member of society, neither man nor woman can be presumed to have consented to . . . uses of the impression of the faces and features upon paper or upon canvas." *Id*. at 219.

62. *See* RESTATEMENT (SECOND) OF TORTS § 652A. *See also* K-Mart Corp. v. Trotti, 677 S.W.2d 632, 636-37 (1984 Tex. App.) (finding that no previously decided Texas case had failed to include the requirement that the intrusion complained of be highly offensive to the reasonable person and that the requirement is one that must be explained to a jury). The court in the *K-Mart* case further held that a failure to include the requirement that the intrusion be highly offensive "would make any wrongful intrusion actionable, requiring a plaintiff merely to establish that the intrusion occurred and that the plaintiff did not consent to it." *Id*. The court stated that the lack of the standard of high offensiveness would "result in fundamentally unfair assessments against defendants who offended unreasonably sensitive plaintiffs, but whose transgressions would not realistically fill either an ordinary person or the general society with any sense of outrage." *Id*.

63. *See* DIAMOND, *supra* note 58, at 438-39.

64. *See* Pearson v. Dodd, 410 F.2d 701, 704 (D.C. Cir. 1969)(finding that an intrusion upon seclusion could occur regardless of whether or not a physical trespass had also occurred).

E. The Right to Privacy in the Private Sector Workplace

The issue of employers intruding into an employee's privacy at the workplace is not new. The technology in the workplace has advanced significantly, making it easier for employers to invade their employees' privacy.[65] The advent and widespread use of the Internet and e-mail in the workplace has created an entirely new context in which employers can and do intrude.[66]

There are areas of an employee's life in which their employer has no legitimate interest or business, and an employer's intrusion into one of these areas may give rise to a cause of action.[67] The method by which an employer conducts an *authorized* inquiry into an employee's private life may be an intrusion upon seclusion if the method results in an overstepping of the employee's privacy or reveals personal matters unrelated to the workplace.[68]

The cases on employer intrusion are broad and cover different types of employer intrusion. An employer will be found to have intentionally intruded upon an employee's privacy only if the employer believed, or was substantially certain that the employer lacked the necessary legal or personal permission to commit the intrusive act.[69] The improper intrusion of an area where the employee has an expectation of privacy alone can raise a right to recover for the intrusion.[70]

In *K-Mart v. Trotti*,[71] the plaintiff complained of an intrusion upon seclusion when store management searched a company owned locker she had locked with her own lock, and the purse inside the locker.[72] The court held that the use of an employer's locker at work, locked with a lock purchased by the employee,

---

65. *See* AMA, *supra* note 4.

66. *Id.*

67. *See, e.g.*, Borse v. Piece Goods Shop, Inc., 963 F.2d 611 (3d Cir. 1992) (explaining that the discharge of an employee who refused to sign a consent form to allow urinalysis screening for drug use and searches of personal property located at the workplace may be an impermissible invasion into the employee's private life). "An intrusion into one of these areas by virtue of the employer's power of discharge might plausibly give rise to a cause of action, particularly where some recognized facet of public policy is threatened . . . ." *Id.* at 614. *See also* Geary v. United States Steel Corp., 456 Pa. 171 (1974) (recognizing that an action for wrongful discharge may be permitted when the firing of an at-will employee violates public policy).

68. *See Borse*, 963 F.2d at 621. *See also* W. PAGE KEETON, DAN B. DOBBS, ROBERT E. KEETON, DAVID G. OWEN, PROSSER AND KEETON ON TORTS (1984).

> Recent cases indicate the existence of two factors in determining whether or not an intrusion which effects access to private information is actionable. First is means used – if it is abnormal in character for gaining access to private information, then the intrusion is likely to be actionable regardless of the purpose. The second is the defendant's purpose for obtaining the information.

Id.

69. *See, e.g.*, O'Donnell v. U.S., 891 F.2d 1079 (3d Cir. 1989).

70. *See* K-Mart Corp. v. Trotti, 677 S.W.2d 632, 637-38 (1984 Tex. App.). The employee had, by purchasing and using her own lock for the employer owned locker, manifested an expectation that the locker be free from intrusion. The employer recognized that manifestation by permitting the employee to purchase and use her own lock. The employer further recognized the employee's manifestation by allowing her to use her own lock when the normal company policy was to distribute company locks while retaining keys or combinations of those locks to enable company interest in maintaining control over the locker and to conduct reasonable searches. Further, the company did not generally give notice of searches as part of the hiring process. *Id.* at 637-38 (*citing* Indus. Found. of the South v. Texas Indus. Accident Bd., 540 S.W.2d 668 (Tex. 1976), Billings v. Atkinson, 489 S.W.2d 858 (Tex. 1973); Trevino v. Southwestern Bell Tel. Co., 582 S.W.2d 582 (Tex. Civ. App. – Corpus Christie 1979)).

71. K-Mart Corp. v. Trotti, 677 S.W.2d 632 (1984 Tex. App.).

72. *See Id.* at 637-638.

with the employer's knowledge, creates an expectation that the locker and its contents will be free from intrusion.[73]

This expectation that a locker will be free from intrusion can be easily carried over to the e-mail context. An individual places private material into a locker, and secures it with a lock, specifically to preclude others from going into the locker and taking what is not theirs. Likewise, an employee-author of an e-mail places private information into the text of an e-mail, and sends it to another person (often via encrypted corporate networks), to be read by the other person. The employee-author protects their e-mail account with a password, to prevent unauthorized intrusions. In this respect, a locker and an e-mail account are very similar – both hold private information and are usually protected by some security device so that others will not breach the privacy. It follows that the level of protection should be similar.

A search of an employee's workspace that reveals matters not related to work may also constitute a common law invasion of privacy.[74] In *Doe v. Kohn Nast & Graf*,[75] an attorney at a large law firm was fired after his receipt at work of a letter from his doctor.[76] The letter had been in the plaintiff's office, but later turned up in the employer's personal file.[77] The letterhead included the terms "Infectious Diseases" and "AIDS Services" and the attorney was demoted within days of his receipt of the letter and was later fired.[78] The *Doe* court left the determination of whether or not an invasion occurred for a jury to decide.[79]

However, some courts have held that where an employee is not found to have a *reasonable expectation of privacy*, an intrusion will not be found.[80] For example, in *O'Bryan v. KTIV Television*,[81] the court held that an employee did not have a reasonable expectation of privacy that no one would search his desk when it was owned by the company, unlocked, in an open accessible area and contained sales information that was the property of the employer.[82] The *O'Bryan* court based its decision on cases in which the employees were government employees and erroneously applied constitutional law.[83] The

---

73. *Id*. at 637-638. Even if the employee failed to lock her locker with her own lock, but instead left the lock open, she has a legitimate expectation to a right of privacy in the contents of and the locker itself. *Id*. *But see* Tapia v. Sikorsky Aircraft Div. of United Tech. Corp., 1998 Conn. Super. LEXIS 1576 (Conn. Super. Ct. 1998) (no published decision) (holding an employer conducted an inventory of a suspended employee's locker was permissible, even though the employer destroyed the plaintiff's personal lock and sorted through the employee's personal belongings).

74. *See* Doe v. Kohn Nast & Graf, P.C., 862 F. Supp. 1310 (D.E. Pa. 1994) ("Doe") (holding that a jury should decide how a copy of the letter from the doctor made its way from the plaintiff's office to his employer's personal file). *See also* Acuff v. IBP, Inc., 77 F. Supp. 2d 914 (D.C. Ill. 1999) (holding that a jury could find that an employer's surreptitious video taping of plaintiff's receiving medical treatment in the on-site nurse's office to be highly offensive to satisfy a claim for intrusion upon seclusion).

75. *Doe*, 862 F. Supp. at 1315.

76. *Id.*

77. *Id*.

78. *Id*.

79. *Id*.

80. *See* O'Bryan v. KTIV Television, 868 F. Supp. 1146 (N.D. Iowa 1994).

81. *O'Bryan*, 868 F. Supp. 1146 (N.D. Iowa 1994).

82. *Id*. at 1159. The court also looked at the fact that the plaintiff could not identify who had searched his desk, and was unwilling to extend the doctrine of *respondeat superior* to the employer where no connection between the search and the employer could be made. *Id*. at 1158.

83. *Id.* at 1158. Specifically, the court looked to *O'Connor v. Ortega*, 480 U.S. 709 (1987) and *Sheppard v. Beerman*, 18 F. 3d 147 (2d Cir. 1994). In *Ortega*, the Supreme Court held that an "employee's expectation

reasonable expectation of privacy standard has no place in the common law. The two standards can and should produce very different results.[84]

Many courts have held that monitoring an employee's personal phone calls without notice will constitute an invasion of privacy, even when no one actually hears or listens to the information.[85] In *Hamberger v. Eastman*,[86] the court held that the tort of intrusion upon seclusion does not require that anyone listen to or hear the recordation.[87] The *Hamberger* court highlighted that an illicitly obtained sound recording carries with it the potential that the recorded conversation will be broadcast in some manner to people other than those involved, and that potential alone impairs an individual's expectation of privacy.[88] Thus, it is not the information that one obtains from such an intrusion that is necessarily tortious, but rather the fact that someone has accessed an area reasonably expected to be private.[89] Likewise, not all content in employee's monitored e-mails is read, sometimes it is simply saved by the company for recordation. In some cases, the monitoring itself will be enough to have violated an employee's privacy.[90]

No finding of intrusion will exist, however, if the employee cannot make a factual showing that there was an actual intrusion upon their phone conversations. This persists even if the plaintiff can prove a related intrusion upon other employee's phone conversations.[91] Most courts have been careful to distinguish between permissible recording of work calls and impermissible recordings of personal calls without notice or permission.[92]

Traditional postal mail has also been held to be a realm into which a private employer may not intrude. In *Doe v. Kohn Nast & Graf*,[93] the defendant law firm opened, and in some cases copied and resealed the plaintiff's personal

---

of privacy must be asserted in the context of the relationship." *Ortega*, 480 U.S. at 717. In *Ortega*, the employer searched the desk and files of Dr. Ortega, a state employee, and several personal items were seized. *Id*. at 712-13. Ortega averred that the search violated the Fourth Amendment. *Id*. at 714. The Supreme Court eventually found that Dr. Ortega had a reasonable expectation of privacy in his desk and filing cabinets, both of which contained items of a personal nature. *Id*. at 718. In *Sheppard*, the Second Circuit held that a law clerk did not have a reasonable expectation of privacy in his office furniture or file cabinets, and that the judge-employer's search of the office was not violative of the clerk's Fourth Amendment rights. *Sheppard*, 18 F.3d at 152. The court's rationale was that the clerk and the judge had an open working relationship and thus the clerk had no reasonable expectation of privacy in his desk or file cabinets. *Id*. at 152.

84. *See infra* § III(C).

85. *See* Hamberger v. Eastman, 106 N.H. 107 (1964). *See also* Marks v. Bell Tel. Co. 460 Pa. 73 (1975) (holding that where there is evidence shown that there is some potential that the recording would be heard in the future, the tort will be established).

86. Hamberger v. Eastman, 106 N.H. 107 (1964).

87. *Hamberger*, 106 N.H. at 112.

88. *Id*.

89. *Id*.

90. *See, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996).

91. *See* Oliver v. Pacific Northwest Bell Tel. Co., 53 Ore. App. 604, 609 (Or. Ct. App. 1981) (holding that the plaintiff's failure to prove that there was any recording or tapping of his phone calls precluded an action for intrusion upon seclusion, even though there was comparable proof of intrusion upon co-worker's phone calls).

92. *See* Ali v. Douglas Cable Communications, 929 F. Supp. 1362, 1382 (D.C. Kan. 1996) (holding the monitoring of business calls at the workplace to be permissible, even where no allowances for personal calls in the workplace were made, and employees were fired in part for making personal calls from their desks). The court also noted that "a reasonable person could find it highly offensive that an employer records an employee's personal phone calls in the circumstances where the employer did not discourage employee's from making personal calls at their desks and did not inform the plaintiff employee that their personal calls would be recorded." *Id*..

93. Doe v. Kohn Nast & Graf, P.C., 866 F. Supp. 190 (D.C. Pa. 1994) ("Doe II").

mail received at the workplace.[94] The plaintiff knew that the firm opened mail addressed to him if the mail might be related to firm business.[95] The court found that an employer is not authorized to open mail addresses to a person at their workplace when the mail appears to be personal.[96]

While cases involving intrusions upon the workplace, mail and phones have generally been found in the employee's favor, almost every case regarding the interception of a private employee's e-mail has found that no intrusion occurred. In *Smyth v. Pillsbury Co*.,[97] the plaintiff, the court found that, under Pennsylvania law, the employee did not have a reasonable expectation to privacy in e-mail communications made voluntarily to his supervisor.[98] The employee was terminated for sending "inappropriate and unprofessional comments" over the corporate e-mail system even though Pillsbury employees had been repeatedly told that all workplace e-mail communications would be kept confidential and privileged.[99] The *Smyth* court held that the company's interest in preventing inappropriate and unprofessional comments over its e-mail system outweighed any privacy interest the employee may have.[100] Further, the court noted that there could be no expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system.[101] This decision is troubling for several reasons. Not only had the employee been repeatedly assured that his e-mails would be kept confidential when they were not, but the court also erroneously applied the Fourth Amendment standard of "expectation of privacy" in a civil, tort-based analysis.[102]

Similarly, in *Bourke v. Nissan Motor Corp*.,[103] the court found that the employees had no reasonable expectation of privacy when they had signed a form that specified that the use of the company computers was for business purposes only.[104] In *Bourke*, one of the plaintiffs' co-workers was conducting a training session, demonstrating the use of e-mail at the workplace.[105] In order

94. *Doe II*, 866 F. Supp. at 195.

95. The plaintiff knew the firm opened personal mail because "the firm had forwarded personal mail mistakenly opened that contained a notification to that effect." *Id*. at 196.

96. *Id*. at 195-96.

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

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

99. *Id*. at 98. Specifically, the employee' e-mails stated that, in reference to the management he wanted to "kill those back stabbing bastards," and referred to an upcoming holiday party as the "Jim Jones Koolaid affair." *Id*. at 98 n.1.

100. *Id*. at 101.

101. *Id*. The court gave no hint to the reasoning that led them to apply the constitutional standard of a reasonable expectation of privacy.

102. *Id*.

103. *See* Bourke v. Nissan Motor Corp., No. B068705 (Cal. Ct. App. filed July 26, 1993) (no published decision), *available at* http://www.loundy.com/CASES/Bourke_v_Nissan.html. Other California cases have led to similar results. In *Flanagan v. Epson* (Cal. App. Dep't. Super. Ct. 1990) (no published decision), an employee brought a class action lawsuit alleging that Epson invaded the employees' privacy by circumventing their passwords and reading their e-mail messages while fostering an atmosphere which led them to believe their messages were private. The *Flanagan* court refused to extend California's right to privacy to employee e-mail, suggesting that such a determination should be left to the legislature. Likewise, in *Shoars v. Epson America*, 1994 Cal. LEXIS 3670 (Cal. 1994) (no published decision), a $ 75 million class action suit for invasion of privacy was dismissed, with the court observing that e-mail privacy is in the province of the legislature.

104. *See Bourke*, No. B068705 at 1.

105. *Id*.

to show how e-mail could be used to aid the management of the dealership, the co-worker randomly selected a message sent by the plaintiff to another employee.[106] The plaintiff's e-mail was of a personal, sexual, nature and not business-related.[107] The co-worker reported this incident to her supervisor, who with management's authorization reviewed the e-mail messages of the entire workgroup.[108] Nissan found substantial numbers of personal, including sexual, messages from the plaintiff, and issued written warnings to plaintiffs for violating the company policy prohibiting the use of the company computer system for personal purposes.[109] The plaintiff filed suit for invasion of privacy.[110]

The *Bourke* court found that, where there was no reasonable expectation of privacy, there can be no violation of a right to privacy.[111] Clearly, the court in *Bourke* failed to note the difference between the Fourth Amendment test and the intrusion upon seclusion test. Having failed to apply the tort's test, the court erroneously concluded that there had been no violation of the employee's privacy.[112]

Some courts have gone so far as to hold that employer monitoring of employee e-mail in a 'personal folder' on a workplace computer is not an invasion of privacy.[113] In *McLaren v. Microsoft*,[114] the court held that Microsoft's review and dissemination of e-mail stored in personal folders on plaintiff's office computer was not an invasion of privacy.[115] Specifically, the court held that the plaintiff had no reasonable expectation of privacy in the contents of e-mail sent over the company e-mail system.[116] Such a holding implies that, since most private employees end their e-mails, personal or private, over company e-mail systems, no employee could possibly have a reasonable expectation of privacy in the content of the e-mail.[117]

Further, the court held that, even if they were to find a reasonable expectation of privacy, no reasonable person would find the invasion of the mailbox to be highly offensive, and the claim would fail regardless.[118] This decision suggests the possibility of zero privacy for the private employee. The *McLaren* court appears to have added an additional burden on the plaintiff by predicating the application of the common law test on the successful passage of

106. *Id*.
107. *Id*.
108. *Id*.
109. *See Bourke*, No. B068705 at 1.
110. *Id*.
111. *Id*. The court specifically and erroneously combined the common law and constitutional causes of action for invasion of privacy and decided both under the constitutional test. *See Bourke*, No. B068705 at 1.
112. *Id*.
113. *See* McLaren v. Microsoft, 1999 Tex. App. LEXIS 4103 (Tex. App. 1999) (holding there was no expectation of privacy where e-mail was stored on the company computer system). *But see* Restuccia v. Burk Tech., Inc., 1996 Mass. Super. LEXIS 367 (Mass. Dist. Ct. 1996) (holding that a question of fact existed as to whether plaintiff had a reasonable expectation of privacy in her e-mail messages and whether the defendant's reading of these messages was an unreasonable interference with that privacy expectation).
114. *McLaren*, 1999 Tex. App. LEXIS 4103 at 1.
115. *Id.* at 1.
116. *Id*. at 13.
117. Note that the standard applied by the court is erroneous; it should be whether or not the invasion would be highly offensive to the reasonable person.
118. *Id*.

the (inapplicable) Fourth Amendment test. This is clearly erroneous and far too heavy a burden to place on the plaintiff.

Additionally, the *McLaren* court's claim that no reasonable person would find the invasion of the 'personal' folder to be highly offensive is an offensive statement in and of itself. The existence of a 'personal' folder intrinsically suggests that individuals will receive and possibly respond to personal mail.[119] To supply an employee with a place to conduct their private affairs at work, and then remove all privacy ensures confusion and non-compliance (whether accidental or intentional) with company policies.[120]

In an extreme example of invasion, an employee was terminated after his private employer learned from his e-mail that he worked as a gay stripper in his off-hours.[121] In *Thomasson v. Bank of America*,[122] the court found that the employee had no reasonable expectation of privacy since a publicity photo of him was posted outside the theatre where he performed.[123] The court further held that the employer did not violate the employee's right to privacy by using information contained in the e-mail as grounds for termination.[124] Not only was the *Thomasson* court's decision discriminatory, it was also flawed. The court applied the wrong standard, using the Fourth Amendment in a case in which there was no state action, rather than the common law cause of action.[125] Further, the *Thomasson* court misapplied the Fourth Amendment test. The Fourth Amendment requires "first that a person [has] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[126] That the employee in *Thomasson* worked as a gay stripper and that his picture was posted outside of the theater in which he worked is of no consequence. A reasonable expectation of privacy must only be found in the e-mail, and the picture posted outside of the theater had no effect on the expectation of privacy in the e-mail. Whether or not a reasonable expectation of privacy could be found in the e-mail alone would be a matter for a trier of fact to decide.[127]

F. Current Standards of Employee Workplace Monitoring

Employees frequently use the Internet and e-mail to complete errands and contact friends and family from work. Most employees do so with the expectation that their privacy will not be invaded, that their communications will not be violated.

---

119. Moreover, the private company in *McLaren* was Microsoft, who likely created the e-mail program that was used by the plaintiff and then encroached upon by the company.

120. This is not to say that all employers do or should prohibit the use of company e-mail for personal purposes, rather that, those companies with policies that prohibit the use of company e-mail for personal activities but supply employees with personal folders on their servers are sending mixed messages to their employees and all but ensuring non-compliance.

121. Thomasson v. Bank of Am., 1995 Cal. LEXIS 1843 (1995) (no published decision).

122. *Id.*

123. *Id.*

124. *Id.*

125. *Id.*

126. *See Katz v. United States*, 389 U.S. at 361.

127. Be that as it may, the Fourth Amendment standard is not the sufficient test under which this case should have been decided.

This leaves employees vulnerable to the rapidly advancing state of technological privacy invasion. Recently, software came onto the market that permits employers to look at the screens of employees as they work.[128] The software, Adavi Silent Watch, is designed to allow an employer to watch what each employee is doing on his or her computer.[129] The software allows the employer to monitor and even freeze remote computers.[130] Employers may also print the contents of a employee's computer screen.[131] Thus employees who used private e-mail accounts in an effort to avoid invasions of privacy fail miserably and are now subject to an even greater scrutiny by their employers.[132]

III. ANALYSIS

G. E-mail Versus Other Forms of Workplace Communication

According to the *Smyth* court, a comment made voluntarily by an employee to a supervisor over the company e-mail system would not be subject to a reasonable expectation of privacy.[133] By extension, any comment made voluntarily by an employee over an e-mail system – and thus any e-mail – would not be subject to any expectation of privacy. There would never be a finding that an employer's reading of employee e-mail would be an intrusion upon seclusion. While e-mail is a means of electronic communication, absent a comprehensive and well-publicized monitoring policy, an employee's reasonable expectation of privacy for electronic communications should not be any different than their expectations for use of the phone or the mails. The fact that employee e-mail is more easily accessible to employers should not be a reason to refuse employees their right to privacy, nor should it give employers leave to monitor their employee's e-mails, covertly or with notice.[134]

E-mail is an entirely different form of communication than traditional devices. E-mail cannot easily be categorized for protection, and its electronic nature makes it vulnerable to attacks of accessibility and ease of interception.

---

128. *See Caught at the Keyboard* (WHDH-TV, 7 News Reports, November 3, 2000), *available at* http://www.whdh.com/news/reports/caught_keyboard.shtml (describing new software available for employers to monitor employee desktops).

129. *See* Adavi, Inc. *at* http://www.adavi.com. ADAVI Silent Watch allows you to control misuse of your computers and restrict objectionable content that may harm or distract others on your computer network. ADAVI Silent Watch will also track computer idle time, record keystrokes, URL logs, monitor incoming and outgoing e-mail and monitor an unlimited number of computers on your network. With ADAVI Silent Watch you can print reports that are date and time stamped, freeze a remote computer, print the contents of a remote computer screen.

130. *See Adavi, Inc., at* http://www.adavi.com. *See also Caught at the Keyboard, supra* note 128.

131. *Adavi, Inc. at* http://www.adavi.com.

132. *Id*.

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

134. The practice of e-mail monitoring would likely be untenable in France, where the "concept of human dignity is more related to notions of community and citizenship than property." *See* Lawrence E. Rothstein, *Privacy or Dignity?: Electronic Monitoring in the Workplace*, 19 N.Y.L. SCH. J. INT'L & COMP. L. 379, 383 (2000). "The worker's dignity is denied when she is treated as a mechanism transparent to the view of others at a distance and therefor manipulable or disposable without the ability to confront the observer." *Id*. at 384. To this end, fundamental rights and liberties cannot be nullified by the worker's consent or be alienated; monitoring must be overt and not hidden. *Id*. at 385.

E-mail cannot accurately be analogized to telephone calls, even though both are forms of electronic communication.[135] Most courts have held that monitoring an employee's personal phone calls at work will constitute an invasion of privacy.[136] Some courts have held that there can be no reasonable expectation of privacy on a cordless phone because the speakers should know that their conversations might be easily intercepted.[137] Often, the basis for the distinction from cord phones has been based upon the ease of interception.[138] A judgement of expectation of privacy should not depend upon ease of interception alone – it is just as easy for the government to tap phone lines and intercept calls on phones with cords as it is for them to do so to cordless phones.[139] Likewise, the ease of interception is a common point of reasoning for judges when they deny privacy protection to employee's whose e-mail has been read by an employer.[140] Most e-mail, however, is sent from one person to another and is not often accidentally intercepted by members of the public in the same manner as cordless telephones.[141] Courts also fail to take into account that e-mail is a written form and has a recorded permanence that telephone conversations lack.[142]

These attributes make e-mail more like traditional postal mail. Courts have held that an employer may not open mail addressed to an employee at the workplace that appears to be personal.[143] In *Vernars v. Young*,[144] a corporate

---

135. *See generally* Scott A. Sundstrom, *You've Got Mail! (And the Government Knows It): Applying the Fourth Amendment to Workplace E-mail Monitoring*, 73 N.Y.U. L. REV. 2064 (1998).

136. *See* Hamberger, 106 N.H. at 112.

137. *See, e.g.*, McKamey v. Roach, 55 F.3d 1236, 1239 (6th Cir. 1995) (holding that interception of conversations made on cordless phone are not subject to ECPA because they are so easily intercepted). Again, no mention is made of the fact that the court has relied upon a Constitutional standard. *See also* In re Askin, 47 F.3d 100 (4th Cir. 1995) (same); Tyler v. Berodt, 877 F.2d 705, 706-07 (8th Cir. 1989) ("Courts have not accepted the assertions of privacy expectation by speakers who were aware that their conversation was being transmitted by cordless telephone."). *But see* United States v. Smith, 978 F.2d 171, 179 (5th Cir. 1992) (noting that changes in technology have made cordless phone conversations more private).

138. *See, e.g.*, *Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, 110 HARV. L. REV. 1591 (1997) "Deciding which expectations of privacy are reasonable . . . requires a judgment about the kind of society in which we want to live. . . . We cannot divorce the level of privacy that the Constitution does protect from a judgment about how much privacy our society ought to protect." *Id.* at 1607.

139. *See Sundstrom*, 73 N.Y.U.L. REV. at 2081.

140. *See generally Smyth*, 914 F. Supp. 97.

141. Victoria A. Cundiff, *Trade Secrets and the Internet: A Practical Perspective*, COMPUTER LAW, Aug. 1997, at 6, 8.

> E-mail transmissions are actually quite secure, even when sent without the aid of encryption software. E-mail is generally more secure from interception than other forms of communication because of the way the Internet works. Information transmitted over the Internet is . . . broken into small 'packets' of data, each of which typically reaches its final destination via a different path. Some packets may travel from New York to Washington via Bangkok, for example, while others may travel through Toronto. These packets are reassembled into a single message only at the end of their travels. The precise route traveled typically varies from message to message. This is part of the reason that the time for e-mail transmission can vary so widely - different messages may arrive by very different routes . . . . This 'packet' transmission method means that, in most cases, e-mail messages are less likely to be readily intercepted than more familiar means of communication.

Id.

142. *See* Parry Aftab, *E-mail & Discovery Considerations*, Leader's Legal Tech Newsl. (N.Y. Law Publ'g Co., New York, N.Y.) May, 1996, at 1 (noting difficulty of deleting e-mail and calling it a 'litigator's nightmare').

143. *See Doe II*, 866 F. Supp. at 196 (holding that a jury could find an intrusion upon seclusion where an employer surreptitiously opened, copied, read and resealed employee's personal mail at the workplace). Even where the employer had established a practice of opening workplace related mail addressed to the employee, opening personal mail was forbidden and could be found to be an intrusion upon seclusion by a jury. *Id.* at

officer opened and read an employee's private mail.[145] The court held that "[j]ust 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."[146] Few courts, however, recognize the analogy between traditional postal mail and e-mail.[147] Because most courts are quick to point out that e-mail is easily accessible and thus the expectation of privacy (or determination of what is highly offensive to the reasonable person) lessened, e-mail must be accorded a higher level of privacy protection.

Courts have also grounded their lack of reluctance to protect employee privacy in the fact that computers used by employees are generally company property and thus the contents of them, including the e-mails sent by employees, are company property as well.[148] The *McLaren* court distinguished e-mail from the locker invasion in the *Trotti* case, stating that "the locker in *Trotti* was provided to the employee for the specific purpose of storing personal belongings, not work items. In contrast, Microsoft provided McLaren's workstation so that he could perform the functions of his job. In connection with that purpose . . . part of his workstation included a company-owned computer that gave McLaren the ability to send and receive e-mail messages. Thus . . . 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."[149]

H. Judicial Confusion and the Need for Clarity

Part of the problem presented to private employees who want to redress an invasion by their employers is the lack adherence to a single type of treatment under the law.[150] Public sector employees have several established routes by which to pursue remedy for an invasion, including Federal statutes and the constitution.[151] Because of the exemptions provided by the ECPA, and the lack of the requisite state action in private employment cases, private employees are essentially limited to the common law.[152] While the dynamism of the common

196.

144. Vernars v. Young, 539 F.2d 966 (3d Cir. 1976) (holding that private individuals have a right to a reasonable expectation that their person mail will not be opened and read by any unauthorized person).

145. *Id.* at 969.

146. *Id.*

147. *See, e.g.*, *Smyth*, 914 F. Supp. 97 (holding that the employee had no reasonable expectation of privacy in the e-mail because the employee made the comments voluntarily over the company e-mail system to his supervisor, and because the company owned the equipment).

148. *See McLaren*, 1999 Tex. App. LEXIS 4103 at 1. *See also Smyth*, 914 F. Supp. at 101.

149. *See McLaren*, 1999 Tex. App. LEXIS 4103 at 1. *See also Smyth*, 914 F. Supp. at 101.

150. The application of the privacy torts varies by jurisdiction. A review of a sampling of intrusion upon seclusion cases to discloses the application of the tort itself. Some states adopt the Restatement definitions verbatim, while others make substantial changes to the tests, requiring a finding of a reasonable expectation of privacy (a constitutional standard) over the Restatement's standard of an invasion highly offensive to a reasonable person. *See, e.g., Smyth*, 914 F. Supp. 97 (applying the constitutional standard of a reasonable expectation of privacy rather than the Restatement's standard requiring an invasion that would be highly offensive to the reasonable person). This point is not meant to be understood as a criticism of the system of common law. Rather, it is an example of when and how the American legal system can fail employees.

151. *See supra* § II B.

152. *See supra* § II B.

law leaves open the possibility for rapid change, it also ensures that employees in Massachusetts will be treated differently from those in every other state.[153] The definitions of intrusion upon seclusion vary from state to state, and thus the likelihood of success on the merit of a claim varies with them.

As evidenced by *McLaren*, *Smyth*, *Bourke*, *O'Bryan* and *Thomasson*, the public/private dichotomy does not preclude judges from confusing the issues.[154] The most striking aspect of a review of cases dealing with an employer wrongfully monitoring an employee's e-mail communication is the almost exclusive application of a constitutional standard of review in place of the traditional tort standard.[155] Of the cases reviewed, no court applied the correct standard by which to find an intrusion upon seclusion in the private workplace.[156] The cases reviewed looked at the invasion under the light of whether or not there existed a reasonable expectation of privacy, the test for the Fourth Amendment, available only for invasions by the state, not invasions by a private employer. [157]

One court chose to review both intrusion and seclusion and violation of the constitutional right to privacy under the constitutional standard as a single claim.[158] One court explained, "Because the constitutional right to privacy is broader than, and encompasses, the common law tort of privacy, we restrict our analysis to a discussion of the constitutional claim."[159] Other cases cited failed to distinguish between the test for an invasion of privacy tort and their application of constitutional invasion of privacy standards.[160] Further, and perhaps most disturbing, all of the reviewed opinions failed to note the fact that the Fourth Amendment test could *not* be applied to a private sector employment case, as the Fourth Amendment applies only to state actions.[161]

The confusion over the applicability of the proper test for an intrusion upon seclusion is sure to be compounded by the ever-increasing use of electronic mail in the workplace. As more and more employers rely upon e-mail as a means of communication for their employees, more and more employers will also monitor that access to protect their corporation. The result will be increased invasions of employee privacy via specialty software, e-mail interception and access to employee e-mail files. Employees will try to redress

---

153. *See* Dorothy Glancy, *At The Intersection of visible and Invisible Worlds: United States Privacy Law and the Internet*, 16 COMPUTER & HIGH TECH. L.J. 357, 380 (2000) (describing the diversity, decentralization and dynamic quality of United States privacy law).

154. *See, e.g.*, *McLaren*, 1999 Tex. App. LEXIS 4103 at 1; *Smyth*, 914 F. Supp. at 101; *O'Bryan*, 868 F. Supp. at 1158; *Thomasson*, 1995 Cal. LEXIS 1843 (no published decision) and *Bourke*, No. B068705, at 1.

155. *See, e.g.*, *McLaren*, 1999 Tex. App. LEXIS 4103 at 1; *Smyth*, 914 F. Supp. at 101 and *Bourke*, No. B068705, at 1.

156. *See, e.g.*, *McLaren*, 1999 Tex. App. LEXIS 4103 at 1; *Smyth*, 914 F. Supp. at 101 and *Bourke*, No. B068705, at 1.

157. *See, e.g.*, *McLaren*, 1999 Tex. App. LEXIS 4103 at 1; *Smyth*, 914 F. Supp. at 101 and *Bourke*, No. B068705, at 1.

158. *See Bourke* at 2.

159. *Id*.

160. In *McLaren*, the court both mentioned and ignored the elements under the cause of action of intrusion upon seclusion. *See McLaren*, 1999 Tex. App. LEXIS 4103 at 3. In *Smyth*, the court examined the plaintiff's reasonable expectation of privacy even though the case was brought as a tort action. *See Smyth*, 914 F. Supp. at 97.

161. *See, e.g.*, *McLaren*, 1999 Tex. App. LEXIS 4103 at 1; *Smyth*, 914 F. Supp. at 101 and *Bourke*, No. B068705, at 1.

the wrong by filing suit for the invasion, and unless courts can either appreciate the different standards or introduce a new remedy, employees will continue to fail in their attempts to protect their privacy.

I. "Reasonable Expectation of Privacy" v. "Highly Offensive to the Reasonable Person"

An important issue is the level of protection afforded by either standard. The Constitutional standard looks at whether the employee has a reasonable expectation to privacy in the monitored activity.[162] The common law privacy tort standard is whether or not the invasion would be highly offensive to the reasonable person.[163] These are very different standards, to be employed in different situations and under different circumstances, and should not be arbitrarily exchanged for the other at the inclination of the judge presiding over the case. The misapplication of these standards has a huge effect.

1. The Reasonable Expectation of Privacy

Certainly, most employees are aware that one's privacy can be invaded on the Internet because of the lengths their employers will go to protect them. Their companies use firewalls that prevent them from accessing certain websites, encryption software to secure the electronic communications the employees send out and receive, and employ the use of passwords to protect vital programs, documents and other information from attack.[164] Moreover, employees and other Internet users are constantly reminded that security is important: the websites they visit and their own employer's corporate policies often stress the importance of on-line security through privacy statements and disclaimers.[165] Internet users are also often aware of the threat that hackers and virus writers pose to their security.[166]

---

162. Katz v. United States, 389 U.S. 347, 361 (1967).

> The reasonable expectation of privacy test has two elements: 'first that a person [has] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' In essence, '[w]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.'

Id.

163. "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another of his private affairs or concerns, is subject to liability to the other for invasion of privacy, if the intrusion would be highly offensive to a reasonable person." RESTATEMENT (SECOND) OF TORTS § 652B (1977). *See supra* note 10.

164. "Firewall" is defined as "any of a number of security schemes that prevent unauthorized users from gaining access to a computer network or that monitor transfers of information to and from the network." THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE (3d Ed. 1992). "Encryption" is "to scramble access codes to (computerized information) so as to prevent unauthorized access." THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE (3d Ed. 1992). To password protect is to employ "an arbitrary string of characters chosen by a user or system administrator and used to authenticate the user when he attempts to log on in order to prevent unauthori[z]ed access to his account." THE FREE ON-LINE DICTIONARY OF COMPUTING, (2000), *available at* http://www.dictionary.com. "A favorite activity among unimaginative computer nerds and crackers is writing programs which attempt to discover passwords by using lists of commonly chosen passwords such as people's names (spelled forwards or backwards)." *Id.*

165. *See, e.g.*, Millennium Pharmaceuticals, Inc. Privacy Policy, *available at* http://www.mlnm.com/privacy_policy.html. *See also* Lycos Network Privacy Policy, *available at* http://www.lycos.com/privacy (providing an in-depth explanation of the Lycos privacy policy, as well as contact information for consumers with privacy and TRUSTe Certification questions).

166. An Internet user is often the first to know of a hack into a high security site, such as the attack on the

Many users are aware of both the inherent security risks in using the Internet and the efforts made by their employers to protect corporate information from attack. Just because employees are aware that their employers have taken protective measures does not necessarily mean that the employee has no reasonable expectation of privacy. Courts are sending the message that ease of access should somehow translate into an employee having no reasonable expectation of privacy because we live in the Internet age, when electronic communications are so prevalent and easily scrutinized.[167]

It appears that opening an employee's private mail received at work, or listening to an employee's private conversations on work phones, or going through an employee's work locker is impermissible, but monitoring an employee's electronic mail, electronic conversations and electronic personal spaces is permissible, simply because they are electronic.[168] The application of the Fourth Amendment test makes these findings easier for the courts, because once they have determined that there is no reasonable expectation to privacy in electronic communication, even if the employer had promised otherwise, there is no recovery for these plaintiffs.[169]

The conclusion that many courts seem to have come to, that there is no reasonable expectation of privacy in electronic communications, is absurd. While employees are or should be aware of their company's monitoring habits, employees should and do have a reasonable expectation of privacy in the content of their e-mails. Just as private employees have a reasonable expectation of privacy in the postal mail they receive at the workplace, they have an equally reasonable expectation of privacy in the electronic mail they receive at the workplace. The difference in procedure of receipt should have no effect on the protections afforded to the employee receiving the letter.

2. Highly Offensive to the Reasonable Person

The intrusion upon seclusion standard should be an easier standard for employee-plaintiffs to meet. Even if courts were to find that no reasonable expectation of privacy could be found in public sector e-mail due to the ease of access to records, any invasion could and should be highly offensive to the reasonable person. Just as the possibility of a home invasion - while perhaps not anticipated by a homeowner - may exist in a homeowner's mind, an actual home invasion is certainly a highly offensive occurrence. Likewise, while private employees may understand that their e-mail could be read, it is an

---

FBI's site on February 18, 2001, because news can be released at great speeds on the Internet. *See, e.g.*, Associated Press, *FBI Admits Its Site Attacked* (Feb. 25, 2000), *available at* http://abcnews.go.com/sections/tech/DailyNews/webattacks000225.html#sidebar. *See also* Ted Bridis, *FBI, Senate Web Sites Hacked*, The Associated Press (May 28, 1999), *available at* http://more.abcnews.go.com/sections/scitech/DailyNews/hackers990528.html. Internet users are also often made aware of virus attacks very quickly, either through the news, corporate concern or even as victims of a virus. *See, e.g.*, Sascha Segan, *Not so Sexy: Don't Click on Kournikova; She's a Virus*, ABCNews.com (Feb. 12, 2001), *available at* http://more.abcnews.go.com/sections/scitech/DailyNews/virus_010212.html (detailing the biggest virus attack in months to hit dozens of major U.S. and European corporations).

167. *See, e.g.*, *McLaren*, 1999 Tex. App. LEXIS 4103 at 1.

168. *See, e.g.*, *McLaren*, 1999 Tex. App. LEXIS 4103 at 1; *Smyth*, 914 F. Supp. at 101; *O'Bryan*, 868 F. Supp. at 1158; *Thomasson*, 1995 Cal. LEXIS 1843 (no published decision) and *Bourke*, No. B068705, at 1.

169. *See, e.g.*, *Smyth*, 914 F. Supp. at 101.

offensive occasion when it actually happens to them, especially if it is monitored in a clandestine way.[170]

Smyth, *Bourke* and *McLaren* prove that not only do courts have little understanding of what constitutes employee privacy in an on-line environment, they also suggest that the very nature of electronic communication is such that no privacy should be expected from it.[171] The innate problem with this view is that it ignores the impact of technology on the world today and in the future.[172] Technology already allows employees to work from home and telecommute into the office site. Some use their personal computers while others use company hardware. The logical extension of the current judicial situation will allow employers to monitor and control what an employee does from the privacy of his or her own home when they telecommute. Some employees who work from home do their work in spurts, interspersing work with pleasure. Employers may ultimately be permitted to spy on these employees during their private and personal time, simply because they do their work on a workplace computer at home.

Certainly, employers have an interest in and a right to protect their companies from tort liability and to ensure the preservation of their intellectual property. Employers must prevent employees from creating situations where the company is open to liability for an act of an employee in the workplace. Likewise, employers must protect their intellectual property from being misappropriated though industrial espionage or hacking. That protection, however, cannot be at the expense of their employee's right to privacy.

3. Looking forward

What can be done to protect the private employee's privacy in the workplace? The current judicial predicament is threatening the already precarious degree of privacy for American employees in both the public and the private sectors. In the private sector, the test of whether or not an intrusion is highly offensive to the reasonable person has been cast aside in preference of the entirely inapplicable Fourth Amendment test of a reasonable expectation of privacy.

Courts must be made aware of this predicament, and their application of the correct tests monitored by students and scholars of the law. Because courts are clearly reluctant to find an invasion of privacy on-line,[173] a fifth invasion of privacy tort must be considered. It must be specific to invasions of electronic communication, just as federal statutes are.[174] It must state a clear and concise

---

170. *See, e.g.*, *Smyth*, 914 F. Supp. at 101. The employee was terminated for sending "inappropriate and unprofessional comments" over the corporate e-mail system even though Pillsbury employees had been repeatedly told that all workplace e-mail communications would be kept confidential and privileged. *Smyth* at 98.

171. *See, e.g.*, *McLaren*, 1999 Tex. App. LEXIS 4103 at 1; *Smyth*, 914 F. Supp. at 101 and *Bourke*, No. B068705, at 1.

172. Additionally, the lack of privacy for employees in the private sector completely disregards the fact that they are living, breathing individuals who deserve at least a basic level of respect from their employers.

173. *See, e.g.*, *McLaren*, 1999 Tex. App. LEXIS 4103 at 1; *Smyth*, 914 F. Supp. at 101 and *Bourke*, No. B068705, at 1.

174. *See* ECPA, 18 U.S.C. §§ 2510-22, 2701-11.

test to avoid the judicial confusion evidenced in the cases already decided.[175] The test could be similar to the current intrusion upon seclusion test, but must take into account the ever evolving state of electronic communications in the modern world. Technology in the year 2001 is not what it was in 1901, or even in the 1990s, and technology will continue to advance, while the individual's privacy rights continue to erode. Courts must recognize, and a new tort must make abundantly clear, that just because the opportunity to monitor employees using new technology is available does not mean that it can be put to indiscriminate use. Not only employees, but all citizens deserve to have their privacy respected by others, whether they are governmental entities or private citizens and corporations.[176]

IV. CONCLUSION

Technology, specifically the Internet, has changed the face of business communication. Where there were once days-long delays in getting materials from offices far away, information can be communicated from a desktop by the click of a mouse. The Internet has created easily accessible, easily traceable, easily monitored forms of electronic communication.[177] As technology advances, employee privacy needs greater protection from the developments that threaten to make the world a very public place. One no longer needs to wait for the postal service to deliver a letter, invoice or report. Communications can be transmitted in milliseconds; invoices sent and received within seconds of purchase; reports sent directly from the word processor on which they were typed.

The state of technology today is bound only to advance to higher levels, and individuals need protection from the dangers that lurk behind that procession. Private sector employees need to be protected as comprehensively as those in the public sector.

Private corporations have almost full reign to monitor employee e-mail. Courts frequently reject employee claims for common law invasion of privacy and continually misapply the law. A common law answer must be developed to protect private employees from intrusions by their employers, now and in the future.

175. *See, e.g.*, *McLaren*, 1999 Tex. App. LEXIS 4103 at 1; *Smyth*, 914 F. Supp. at 101; *Bourke*, No. B068705, at 1.

176. Clear and continuous notice requirements should be a condition for employers who choose to monitor their employees at work. A signature on a piece of paper presented with many others at an employee's corporate orientation should not be sufficient. Employers should be required to post their policies in employee common areas and practice continuous forms of notice such as reminders at company meetings, corporate policy e-mails and proof of verbal explanation of a policy at orientation. While this may seem to be a hefty requirement to force upon corporate America, it would probably be easier and cheaper than a lawsuit.

177. *See* AMA, *supra* note 4 (measuring time logged on, keystroke counts and url logs.).

THIS PAGE INTENTIONALLY LEFT BLANK