

1984 IS STILL FICTION: ELECTRONIC MONITORING IN THE WORKPLACE AND U.S. PRIVACY LAW

CHRISTOPHER PEARSON FAZEKAS¹

ABSTRACT

Electronic monitoring in the workplace has been the subject of relentless public criticism. Privacy advocates argue that technological advancements have given overbearing employers powerful tools to abuse employee dignity in the name of productivity and that new legislation should bolster workplace privacy rights. This iBrief contends that current U.S. legal doctrine governing electronic monitoring in the workplace is fair given the nature and purpose of the workplace, and potential employer liability for employee misconduct.

INTRODUCTION

¶1 Technology continues to make the world a smaller place; it is easier to keep in touch with people than ever before. This is not an entirely positive development, however. The ease with which individuals' personal information may be recorded, documented, identified and produced is a controversial issue. For example, significant debate has centered on the Federal Bureau of Investigation's Carnivore Project which has the capacity to monitor millions of electronic communications worldwide.² Even the use of traffic cameras to monitor public intersections, where no one has an expectation of seclusion, is to some an invasion of privacy.³

¶2 This debate is especially intense in the context of electronic monitoring in the workplace.⁴ Should employees have a right to Internet

¹ J.D., LL.M., Duke University School of Law, May 2004; B.A., University of Virginia, May 2001. The author is currently practicing law in New York City.

² See, e.g., Erich Luening, *FBI Takes the Teeth Out of Carnivore's Name*, CNET NEWS.COM, Feb. 9, 2001 at http://news.com.com/FBI+takes+the+teeth+out+of+Carnivores+name/2100-1023_3-252368.html (explaining that Carnivore has engendered so much public controversy that the FBI has now changed the program's name to DCS1000) (last visited Oct. 26, 2004).

³ See, e.g., John Martin, *Caught Red Handed*, ABCNEWS.COM, May 23, 2003, at http://abcnews.go.com/sections/wnt/WorldNewsTonight/wnt010523_running_relights.html (last visited Sept. 22, 2004)

⁴ Hereinafter, the term "Internet" also includes email transmissions that occur over local office "intranet" networks. While it is possible that fine distinctions

access free from employer supervision? In the United States, the law has not recognized a strong right to privacy for employee Internet use. This reality has driven many to argue for a reallocation of legal rights. Some assert that employees' privacy rights in the work place should be bolstered with additional statutory protections to preserve employees' sense of dignity.⁵ Others seek the development of an entirely new privacy regime.⁶

¶3 This iBrief argues that changing the law governing workplace privacy is unnecessary. The current law in this area is sufficiently dynamic to incorporate technological advances and represents an equitable distribution of the legal rights and obligations of all parties concerned. Although employees have little legal protection while perusing the Internet or communicating by email at work, this minimal degree of protection is commensurate with the nature and purpose of the workplace and the substantial liability employers face for employee misuse of the Internet. Moreover, employers are unlikely to abuse their monitoring privilege, as it is in their best interest to balance surveillance needs with employee quality

may be drawn between the "Internet" and an "intranet" under federal and state wiretap statutes, the author is of the belief those distinctions will not significantly affect judicial outcomes.

⁵ See, e.g., Peter J. Isajiw, Comment, *Workplace E-mail Privacy Concerns: Balancing the Personal Dignity of Employees with the Proprietary Interests of Employers*, 20 TEMP. ENVTL. L. & TECH J. 73, 74 (2001) ("[S]tatutory intervention seems the only means to protect individual human dignity and privacy in e-mail accessed at work."); S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace*, 32 GA. L. REV. 825, 848 n.89 (1998) (summarizing various law review articles that argue for changes ranging from an amendment to the Electronic Communications Privacy Act of 1986 to new workplace privacy legislation). The issue is certainly one that is international in scope. See, e.g., Robert Muckle, *Email Monitoring in the Workplace: A Simple Guide to Employers* (July 2003), at http://www.pythagoras.co.uk/file_attachments/mai/Email_in_the_Workplace.pdf (last visited Sept. 22, 2004), (discussing The Employment Practices Data Protection Code released in June 2003 in the United Kingdom); Privacy Amendment (Private Sector) Act of 2000, No. ___ 2000, available at <http://parlinfoweb.aph.gov.au/piweb/Repository/Legis/oldBills/Linked/23010112.pdf> (last visited Sept. 22, 2004) (Australian Act expanding the 1988 Privacy Act to govern the manner of collecting, recording, and transferring employees personal information revealed in electronic surveillance).

⁶ See, e.g., Wilborn, *supra* note 5, at 830-31 (advocating the elimination of the "anachronistic inequality" created by maintaining a distinction in individual privacy protection afforded employees in public and private sector workplaces); Donald R. McCartney, Comment, *Electronic Surveillance and the Resulting Loss of Privacy in the Workplace*, 62 UMKC L. REV. 859, 891 (1994) ("[L]egislation needs to be enacted that provides a generalized protection for the right to privacy.").

of life and because employer misuse of personal information is prohibited by a variety of existing legal doctrines.

I. EMPLOYEES' RIGHT TO INTERNET PRIVACY IN THE WORKPLACE

¶4 As currently applied, federal law affords employees little protection from electronic monitoring. Internet monitoring, including local network email monitoring, has been attacked by employees primarily on two theories: first, as an unlawful interception of a wire communication or unauthorized wiretap; and second, as an invasion of privacy.⁷

¶5 Challenges to electronic monitoring by employers based on unauthorized wiretaps typically fail because the state or federal wiretap statute is inapplicable to email monitoring, or because the particular manner by which employers monitor the communication is outside the scope of the statute.⁸ The statute most frequently at issue has been the 1986 Federal Electronic Privacy Communications Act ("EPCA"). The EPCA does not prohibit interceptions of electronic communications made in the ordinary course of business for the purpose of protecting the rights or property of the network provider, as well as interceptions made with the consent of the sender or recipient.⁹ Thus, those companies that monitor their networks to

⁷ Invasion of privacy is sometimes more narrowly presented as a cause of action for "intrusion upon seclusion." Invasion of privacy is often considered to include other causes of action such as public disclosure of private facts.

⁸ See *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 635 (E.D. Pa. 2001) (finding that no interception had occurred under the EPCA where the email was reviewed by the company in its post-transmission storage bank after transmission to the intended recipient was complete); *Wesley College v. Pitts*, 974 F. Supp. 375, 384 (D. Del. 1997) (finding that the EPCA requires an email to be intercepted while in transit and does not include reading an email off of a computer screen); *Restuccia v. Burk Technology, Inc.*, 1996 Mass. Super. LEXIS 367, *4—*6 (Mass. Super. 1996) (finding that a Massachusetts wire tap statute clearly permitted the retention of emails in a back up system because the system met the exception for an intercommunication device used in the ordinary course of business); C. Forbes Sargent, III, *Electronic Media and the Workplace: Confidentiality, Privacy, and Other Issues*, 41 BOSTON B.J. 6, 19 (1997) (citing *Flanagan v. Epson America*, an unpublished opinion of the California Court of Appeals that held the California wire tap law covered telephone conversations, not email).

⁹ See 18 U.S.C. §§ 2510-2710 (2000). The EPCA is notably ambiguous. See *Fraser*, 135 F. Supp. 2d at 633, though it is clear "network providers" has been deemed to include employers. See *U.S. v. Mullins*, 992 F.2d 1472, 1478 (9th Cir. 1993) (finding an airline to be a service provider of its reservation network and therefore exempted from the ECPA for actions taken in the ordinary course of business to protect the airlines rights or property). The meaning of "ordinary course of business" has been more elusive, however. See *Adams v. City of Battle Creek*, 250 F.3d 980, 984 (6th Cir. 2001) ("Ordinary course of business"

protect their interests, or do so with employee consent, have a strong argument that they are exempt from federal wire tap regulation.

¶6 Invasion of privacy is a more potent ground on which employees object to Internet monitoring. A right of privacy generally extends to employees in the workplace. This right is, however, typically limited to those instances where the matter intruded upon is “intensely private.”¹⁰ Thus, where an employer videotapes an employee’s medical examination in her office¹¹ or reads personal medical documents on an employee’s desk,¹² a jury may be permitted to hear the issue. However, the nature of the workplace is generally a public one and an employee is hired for the purpose of attending to company business, not personal matters. Therefore, courts tend to reject most employees’ privacy claims on the basis that there was no reasonable expectation of privacy.¹³

¶7 The public nature of the workplace has led many courts to find that no right of Internet privacy exists at work. The Restatement (Second) of Torts declares: “One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.”¹⁴ In applying this standard, courts have most commonly found monitoring of employee Internet use not to be an invasion of privacy for two reasons: first, employees have no reasonable expectation of privacy for communications voluntarily transmitted on an employer’s network; and second, even if there were a reasonable expectation of privacy, the intrusion upon seclusion is not highly offensive. The courts have reached similar conclusions even when no notice of employer monitoring was provided to the employee.

is not defined in the statute, but it generally requires that the use be (1) for a legitimate business purpose, (2) routine and (3) with notice. There is some disagreement in the case law about whether ‘covert’ monitoring can ever be in the ‘ordinary course of business.’”). For a more extensive review of the law in this area *see* Isajiw, *supra* note 5, at 81-89.

¹⁰ *See* Joan T.A. Gabel & Nancy R. Mansfield, *The Information Revolution and Its Impact on the Employment Relationship: An Analysis of the Cyberspace Workplace*, 40 AM. BUS. L. J. 301, 313 (2003) (“[B]ecause courts have recognized a diminished expectation of privacy in the workplace, claims for this tort typically lie only where the matter intruded upon is intensely private.”).

¹¹ *See* *Acuff v. IPB, Inc.*, 77 F. Supp. 2d 914 (C.D. Ill. 1999).

¹² *See* *Doe v. Kohn Nast, & Graf, P.C.*, 862 F. Supp 1310, 1326 (E.D. Pa. 1994).

¹³ *See* Gabel and Mansfield, *supra* note 10 and accompanying text; Isajiw, *supra* note 5, at 74 (“[Y]ears of precedent, including recent decisions, have construed this right too narrowly in the context of employer/employee relationships.”).

¹⁴ RESTATEMENT (SECOND) OF TORTS § 652B (1976).

¶8 In *Smyth v. Pillsbury Co.*,¹⁵ a federal district court conclusively rejected the argument that email monitoring by the employer constitutes an invasion of privacy.¹⁶ In the case, the employee plaintiff had been assured that the content of monitored emails would remain confidential and would not be used against employees for termination or reprimand, although the employee was advised that the email privilege should not be abused.¹⁷ After the employer reviewed multiple emails that contained offensive commentary about the employer, the employee was terminated for abusing the email privilege by sending too many emails.¹⁸ Granting summary judgment, the court held, “[O]nce plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost.”¹⁹ The court also found that the interception of emails was not highly offensive.²⁰

¶9 Supporting these conclusions, the court emphasized the voluntary nature of the communication and the company’s interest in providing a safe work environment.²¹ Because the emails were sent voluntarily, the facts at hand could be distinguished from those cases where employees were required to disclose personal information. Greater scrutiny would be warranted, for instance, when as a condition to continued employment an employee submits to a urinalysis test or search of their personal property.²² In recognizing an employer’s substantial liability for employee Internet use, the court further asserted, “[T]he company’s interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments.”²³

¶10 The precedent established by *Smyth* does not mean that monitoring an employee’s Internet use may never be considered an invasion of privacy.²⁴ For example, in another 1996 case, *Restuccia v. Burk*

¹⁵ 914 F. Supp. 97 (E.D. Pa. 1996).

¹⁶ *Id.* at 101.

¹⁷ *Id.* at 98.

¹⁸ *Id.*

¹⁹ *Id.* at 101.

²⁰ *Id.*

²¹ *Id.*

²² *Id.*

²³ *Id.* (emphasis added).

²⁴ See *Kelleher v. City of Reading*, No. 01-3386, 2002 U.S. Dist. LEXIS 2408, at **24—25 (E.D. Pa. May 29, 2002) (“*Smyth* . . . do[es] not necessarily foreclose the possibility that an employee might have a reasonable expectation of privacy in certain e-mail communications, depending upon the circumstances of the communication and the configuration of the e-mail system.”).

Technology, Inc.,²⁵ a Massachusetts superior court found that where two employees were not informed that their email could be accessed by others and their computer accounts were protected by individual passwords, a claim of invasion of privacy would survive summary judgment.²⁶ Other cases generally support the holding in *Smyth*. Even in those instances where no notice was provided to the employee that monitoring would occur²⁷ or when the employee was convinced that the employer provided him space to shelter emails from management's purview, there is not necessarily a reasonable expectation of privacy.²⁸ Where the employee has constructive notice that his or her emails are subject to management's review, courts have unanimously found monitoring not to be an invasion of privacy.²⁹

¶11 Therefore, an invasion of privacy claim against an employer for monitoring employee Internet use is unlikely, and is almost certainly proscribed if the employer has given the employee notice.³⁰ This allocation of legal rights, which appears to favor the employer, has been attacked from

²⁵ 1996 Mass. Super LEXIS 367.

²⁶ *Id.* at **2—3, 9. The continued relevance of the *Restuccia* decision is questionable, however. The opinion quickly disposed of the issue without inquiring into precedent, and a more recent case in the Federal District Court for Massachusetts contradicts the holding. See *Garrity v. Hancock Mut. Life Ins. Co.*, No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343, at *6 (D. Mass. May 7, 2002).

²⁷ See *Id.*; *Kelleher*, 2002 U.S. Dist. LEXIS 2408 at **25—26; *McClaren v. Microsoft Corp.*, No. 05-97-00824-CV, 1999 Tex App. LEXIS 4103, at *13 (Tex. Ct. App. May 28, 1999).

²⁸ See *McClaren*, 1999 Tex App. LEXIS 4103 at **4—13.

²⁹ See *Garrity*, 2002 U.S. Dist. LEXIS 8343, at **2—5 (finding that Plaintiff forwarded jokes clearly with the expectation that they would be shared); *Kelleher*, 2002 U.S. Dist. LEXIS 2408, at *25 (finding that no reasonable expectation of privacy could exist where the City Guidelines specifically informed employee that no expectation of privacy should exist.).

³⁰ Collateral actions predicated upon an invasion of privacy, such as wrongful discharge, fail on the same grounds. See *Garrity*, 2002 U.S. Dist. LEXIS 8343 at *9 (finding a wrongful discharge claim predicated upon employer monitoring of email duplicative of privacy and wire tap claims and misplaced); *Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 100—01 (E.D. Pa. 1996) (finding that because the employer did not tortuously invade the employee's privacy, it could not have been have violated public policy by dismissing him on account of the information revealed by employer's monitoring). Cf. *Restuccia*, 1996 Mass. Super. LEXIS 367 at **9—10 (rejecting Defendant's motion for summary judgment on plaintiff's claim for wrongful termination where the claim was based on plaintiff's claim for invasion of privacy that had been permitted to proceed to trial).

all sides by commentators concerned about privacy and dignity. The current legal doctrine is, however, entirely fair and reasonable.

II. MONITORING EMPLOYEE USE OF THE INTERNET IS REASONABLE

¶12 The minimal privacy protection afforded employees is fair and reasonable given the nature and purpose of the workplace, and the substantial liability employers face for employee Internet use.

¶13 The workplace is generally not a private place. In the seclusion of one's home there is a well-established and legally protected expectation of privacy from other persons.³¹ However, upon leaving one's private residence and entering premises possessed by another, expectations of privacy are drastically reduced because one occupies property over which one does not exercise complete dominion.³² An expectation of privacy can be otherwise established by contract or substantiated where the premises are intensely private such as a locker room, hotel bedroom, or office restroom.³³ Nevertheless, such cases are the exception rather than the norm. An employer's facilities are predominantly public in nature because they are not directly owned by the employee and they are shared with others.

¶14 The lack of privacy in the workplace is particularly justifiable because occupation by an employee of the premises is conditioned on using those premises to achieve employer goals. Employees are provided certain tools by the employer—for instance, a phone, voicemail, email and Internet access—principally because those items help the employee achieve a business objective. It is here, however, that many supporters of increased employee privacy rights make their stand. They contend that the increased productivity demands of the workplace require employees to mingle the personal and the professional, especially when it comes to such items as phone, email or Internet usage, and that the law in this area should

³¹ See Isajiw, *supra* note 5, at 93 (commenting that notions of privacy in the United States are intricately tied to conceptions of personal property thus “the sphere of control that is privacy is commonly associated with a person's home or marital relationship”). See also Wilborn, *supra* note 5 (arguing that the public/private distinction granting government employees greater privacy rights is a false distinction and should be amended).

³² This connection between proprietary interests and privacy is well-established in the U.S. legal tradition. *Id.*

³³ See, e.g., *Doe by Doe v. B.P.S. Guard Services, Inc.*, 945 F.2d 1422, 1427 (8th Cir. 1991) (affirming verdict for Plaintiff where the changing room for fashion show models was monitored by video surveillance). Some states specifically forbid monitoring of certain areas. See, e.g., *Adams v. Oak Park Marina*, 261 A.D.2d 903, 904 (N.Y. App. Div. 1999) (finding that New York's General Business Law §395-b prohibits the installation of a video camera in a bathroom).

recognize such a real workplace dynamic.³⁴ Employees are going to take care of personal business in the office because it is necessitated by circumstance and if the employee can most quickly resolve the personal matter by using workplace resources it also inures to the employer's benefit.³⁵ In such an environment, where employees' handling of intensely private matters results in a benefit to the employer in terms of increased morale and productivity, employees arguably should not be forced to sacrifice their privacy rights.

¶15 This argument is valid so long as employees do not abuse the privilege. Unfortunately, the privilege is commonly abused. One recent study found that employees use the Internet 75.5% of the time for their work and 24.5% of time for personal reasons such as reading the news, viewing pornography, day trading and keeping up on sports scores.³⁶ Shirking did not begin with the creation of the Internet, of course. Before the Internet, employees wasted time by the water cooler or in the smoke room. The difference is that those environments were easily monitored without the aid of surveillance software. There is some sense of seclusion in one's use of the Internet because it usually takes place at an individual terminal. However, if an employer is entitled to measure the effort employees put into their work, then monitoring Internet usage should be reasonably expected by all employees and even welcomed by some.³⁷

¶16 Employee misuse of the Internet can also result in substantial legal liability for the employer.³⁸ Under the doctrine of *respondeat superior*, an employer may be held liable for the actions of an employee committed within the scope of employment or in furtherance of the employer's

³⁴ See Isajiw, *supra* note 5, at 94.

³⁵ *Id.*

³⁶ Regina Lynn Preciado, *Mouses to the Grindstone*, WIRED NEWS, Aug. 12, 1998, at <http://www.wired.com/news/culture/0,1284,14371,00.html> (last visited Sept. 22, 2004).

³⁷ Individuals whose work cannot be adequately measured by output, but requires some recognition of effort, should in many instances favor monitoring.

³⁸ This reality has been noted by a number of courts to support their dismissal of invasion of privacy claims for Internet surveillance. See *Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 1001 (E.D. Pa. 1996) (“[T]he company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments.”); *McClaren v. Microsoft Corp.*, No. 05-97-00824-CV, 1999 Tex App. LEXIS 4103, at *13 (Tex. Ct. App. May 28, 1999) (“[T]he company's interest in preventing inappropriate and unprofessional comments, or even illegal activity, over its e-mail system would outweigh [the plaintiff's] claimed privacy interest in those communications.”).

interest.³⁹ While “scope of employment” could be interpreted narrowly, vicarious liability of an employer for the actions of her employees has been and continues to be interpreted broadly.⁴⁰ So long as an employee’s wrongful act is closely connected to a work activity, the scope of employment condition is likely met.⁴¹ Even if the employee engages in an activity specifically forbidden by the employer, so long as he was carrying out job responsibilities, the employer will probably be liable.⁴² Thus, an employer will likely be liable in those instances where an employee commits a foreseeably wrongful act during regular business hours in an office provided by the employer.⁴³ This broad interpretation is even more daunting to an employer-defendant because the employer bears the burden

³⁹ N. PETER LAREAU, LABOR AND EMPLOYMENT LAW § 270.01[1] (2004). The Restatement (Second) of Agency states that:

- (1) Conduct of a servant is within the scope of employment if, but only if:
 - a) It is of the kind he is employed to perform;
 - b) It occurs substantially within the authorized time and space limits;
 - c) It is actuated, at least in part, by a purpose to serve the master; and
 - d) If force is intentionally used by the servant against another, the use of force is not unexpected by the master.
- (2) Conduct of a servant is not within the scope of employment if it is different in kind from that authorized, far beyond time or space limits, or too little actuated by a purpose to serve the master.

RESTATEMENT (SECOND) OF AGENCY § 228 (1958).

⁴⁰ LAREAU, *supra* note 39, at § 270.01[1].

⁴¹ *Id.*

⁴² *Id.*

⁴³ *See, e.g., Doe v. United States*, 912 F. Supp. 193, 194 (E.D. Va. 1995) (finding that a hospital employer liable for sexual assault of a patient by a doctor because the act occurred during regular hours, in an office provided by the hospital, and patient abuse was foreseeable). Other courts have gone even further in drawing employees’ actions into the scope of employment. For instance, in *Goff v. Teachers’ Retirement Sys.*, 713 N.E.2d 578 (Ill. App. Ct. 1999), an Illinois appellate court ruled that an act occurred in the scope of employment if “its origin is in some way connected with the employment so that there is a causal connection between the employment and the . . . injury.” *Id.* at 582. Similarly, in *Davis v. Liberty Mutual Ins. Co.*, 19 F. Supp. 2d 193 (D. Vt. 1998), a Vermont federal district court determined that conduct falls within the scope of employment “when it occurs within a period of time when the employee is on duty and in a place where the employee may reasonably be expected to be while fulfilling the duties of his or her employment contract.” *Id.* at 197.

of showing that an act was outside the scope of employment.⁴⁴ Therefore, employee claims will often survive summary judgment and exponentially increase the cost and risk of litigation to the employer. Some courts have been more willing to declare that an employee was off on a “frolic of his own” as opposed to acting in the scope of employment; however, for employers seeking to operate safely within the confines of the law, judicial uncertainty favors conservatism and justifies supervision.

¶17 The potential for employer liability to third persons arising out of unlawful employee conduct on the Internet is significant. The Internet is a powerful instrument with which employees can commit numerous illegitimate or unlawful acts. Not only can employees communicate with each other beyond the view of managers, they can also communicate with the entire World Wide Web without management’s notice. Defamation, public disclosure of private facts, false light, intentional infliction of emotional distress are all causes of action easily satisfied by an employee’s publication of information to the web. Trade secrets and patents belonging to a client also are easily ruined by Internet transmission. These causes of action are in addition to spamming, computer fraud and other computer-oriented abuses. Many of these Internet offenses will likely be based upon facts that bring the conduct within the scope of employment. They can be committed during regular work day hours by an employee using the Internet under the auspices of performing work-related tasks, on a network and computer provided by the employer, and it is entirely foreseeable that that these privileges are subject to employee abuse in many different ways.

¶18 Moreover, employers are liable in some cases even for those acts committed by its employees outside the scope of employment. Generally, an employer has a duty to ensure a safe working environment and the safety of those who will foreseeably come into contact with its employees.⁴⁵ The doctrine of negligent retention may result in employer liability if an employer knew or should have known that an employee was unfit to carry out his duties.⁴⁶ An employer is also liable for an employee’s conduct if that employee used his actual or apparent authority to commit a wrongful act.⁴⁷ Most significantly, violations by employees of anti-discrimination statutes like Title VII of the Civil Rights Act of 1964,⁴⁸ the Americans with Disabilities Act,⁴⁹ and the Age Discrimination in Employment Act⁵⁰ can

⁴⁴ See *Doe*, 912 F. Supp. at 194.

⁴⁵ LAREAU, *supra* note 39, § 270.03[4].

⁴⁶ *Id.* § 270.03[3][c].

⁴⁷ *Id.* § 270.03[5][a].

⁴⁸ Pub. L. No. 88-352, 78 Stat. 241 (1964).

⁴⁹ Pub. L. No. 102-569, 106 Stat. 4344 (1992)

⁵⁰ Pub. L. No. 90-202, 81. Stat. 602 (1967).

result in substantial liability for an employer.⁵¹ Title VII involves the greatest potential liability for most employers. While the Supreme Court has found sexual harassment to fall outside the scope of employment, if an act is committed by a supervisor⁵² and involves a “tangible employment action” against the complaining employee such as termination, reassignment with significantly different responsibilities, or a significant change in benefits, a violation will be deemed to have occurred.⁵³ Absent an employer’s ability to establish that it took reasonable care to prevent or correct the wrong and that the employee failed to avail herself of the employer’s remedial measures, the employer will be held liable for the supervisor’s actions and possibly subjected to punitive damages.⁵⁴

¶19 Therefore, to the extent that an employee’s use of the Internet falls outside of the scope of employment, causes of action may arise for breach of an employer’s general duty of care, under the doctrines of negligent retention or actual or apparent authority, or under various statutory sections like Title VII. Negligent retention, in particular, presents an interesting dilemma for employers. An employer may be held liable for an employee’s acts if the employer “should have known” what the employee was doing. Therefore, if monitoring an employee’s Internet activity is a common and cost efficient method of supervision, the failure to implement such an electronic surveillance system could be used against the employer.⁵⁵ For example, a Wall Street firm was recently fined for failing to monitor instant messages sent between traders.⁵⁶ An employer’s general duty of care may

⁵¹ LAREAU, *supra* note 39, at § 270.04[1]. The precedents set out for harassment claims under Title VII have been widely read into anti-discrimination statutes as well. *Id.*

⁵² Employers are held liable for acts committed by co-workers only if they knew or should have known about the conduct and failed to remedy the improper conduct. *Id.* § 270.04[2].

⁵³ *Id.* § 270.04[3].

⁵⁴ *Id.* §§ 270.04[4]—.05. The landmark Supreme Court decision governing the assessment of punitive damages in Title VII claims is *Kolstad v. Am. Dental Ass’n*, 527 U.S. 526 (1999). The Court held that “in the punitive damages context, an employer may not be vicariously liable for the discriminatory employment decisions of managerial agents where these decisions are contrary to the employer’s ‘good-faith efforts to comply with Title VII.’” *Id.* at 545 (quoting *Kolstad v. Am. Dental Ass’n*, 139 F.3d 958, 974 (D.C. Cir. 1998) (Tatel, J., dissenting)).

⁵⁵ *But see* *Blakey v. Continental Airlines*, 751 A.2d 538, 551 (N.J. 2000) (holding in the context of a Title VII sexual harassment suit that employers do not have a duty to monitor employee’s mail).

⁵⁶ Nand Mulchandani, *Workplace Monitoring: How to Protect Yourself*, TECHTV.COM, at http://www.g4techtv.com/callforhelp/features/37738/Workplace_Monitoring_How_to_Protect_Yourself.html (last visited Apr. 27, 2004).

also give rise to the same conflict. Title VII claims of harassment and discrimination have already been an area flush with litigation over employer liability for employee emails. Emails are often cited in the complaint and accepted as evidence of harassment and discrimination.⁵⁷

¶20 The potential for employer liability to third persons injured by its employee's Internet use is not the limit of damage that can be caused by an employer's failure to monitor electronic activity in the workplace. Great damage can be caused to the employer's own operations. Given their actual or apparent authority, employees may have the ability to bind the corporation to unwanted contracts or be officially quoted by the press on an unapproved topic. Similarly, trade secrets, patents and business models and plans may be distributed without management's notice.

¶21 Hence the workplace is more public than private, and most assuredly, it is a place for work. The ease with which the Internet provides employees a mechanism for shirking their responsibilities and engaging in illicit activities warrants employer monitoring of electronic activity. Regulators have recognized that the substantial liability employers bear for their employees' acts requires this supervision. Even the Equal Employment Opportunity Commission specifically recommends that employers closely monitor employee conduct to mitigate their liability for harassment and discrimination.⁵⁸ While some may view monitoring as an intrusion meant to assert even greater control over employees, for most employers Internet surveillance stems from their basic responsibility to ensure a safe workplace for their employees and the public at large. Indeed, employers have a number of incentives to ensure that they do not abuse their right to monitor.

⁵⁷ See, e.g., *Blakey*, 751 A.2d at 551—52 (holding that postings on an electronic bulletin board may be sufficient to establish employer liability for harassment); *Strauss v. Microsoft Corp.*, 814 F. Supp. 1186, 1188-89 (S.D.N.Y. 1993) (finding that supervisor's behavior both in person and in email communications was sufficient for a jury to find gender discrimination); *Petersen v. Minneapolis Cmty. Dev. Agency*, 1994 WL 455699, *2 (Minn. Ct. App. Aug. 23, 1994) (finding that harassing emails that continued even after unwelcome physical advances stopped were sufficient to support plaintiff's claim of sexual harassment); Ann Carrns, *Prying Times: Those Bawdy E-mails Were Good for a Laugh-Until the Ax Fell*, WALL ST. J., Feb. 4, 2000, at A1 (noting that Chevron settled with four employees for \$2,200,000 for harassment claims that included the circulation of chauvinistic jokes by employees). Cf. *Schwenn v. Anheuser Busch, Inc.*, 1998 WL 166845, *4 (N.D.N.Y. April 7, 1998) (finding email messages sent to the plaintiff not sufficiently severe or pervasive to establish liability).

⁵⁸ LAREAU, *supra* note 39, at § 270.03[4] (citing EEOC Enforcement Guidance, "Vicarious Employer Responsibility for Unlawful Harassment by Supervisors," June 18, 1999).

III. EMPLOYERS ARE UNLIKELY TO ABUSE THEIR RIGHT TO MONITOR

¶22 While some commentators take a principled stand and reject all employer monitoring of employee Internet use, many would agree that if the sole motivation for monitoring employees' Internet usage was to detect crimes and maintain a safe and respectable work environment, an employer's right to monitor electronic activity would be less objectionable. Thus the right itself is not as objectionable as the potential for that right to be abused. Many commentators fear that employers may use their ability to monitor to turn the workplace into an "electronic sweatshop" or use the information obtained through their surveillance to the detriment of the employee.⁵⁹ These fears are reasonable given the fact that employers typically possess substantial bargaining power. Anecdotal evidence of employee monitoring at its worst includes stories about an employees being fired for inappropriate comments about a supervisor in emails to co-workers, chair devices that monitor worker "wiggling" in the belief that more wiggling means less work, and employer monitoring of bathroom use that includes publication of a schedule of total bathroom minutes per employee.⁶⁰ However, employers actually have little incentive to abuse their monitoring privilege because it does not promote a productive work environment. Moreover, if information gathered through electronic monitoring were improperly handled, the employer could very well be subject to substantial liability.

¶23 As discussed in Part II, monitoring employee Internet use is one tool to prevent shirking. Where extended water cooler stops and smoke breaks are easily identified and checked, it is far more difficult for the employer to determine whether an employee is actually being productive while using the Internet, especially if the difficulty of the task varies or an employee's contribution is not able to be easily identified. Thus, electronic monitoring software that records and consolidates information on how that employee is using her computer helps overcome this information asymmetry. Of some objection is the fact that electronic monitoring is so comprehensive that every detail is recorded. As one commentator asserts: "Worst of all, the supervisor isn't even human. Employees must labor at top speed under the view of unwinking computer taskmasters that record every item of work completed, along with every mistake, rest break and deviation from standard practice."⁶¹ The fact that an Internet monitoring

⁵⁹ See, e.g., Paul Atwell, *Big Brother and the Sweatshop: Computer Surveillance in the Automated Office*, 5 SOC. THEORY 87 (1987).

⁶⁰ See Wilborn, *supra* note 5, at 825.

⁶¹ See FINKIN, ET AL., LEGAL PROTECTION FOR THE INDIVIDUAL EMPLOYEE 224 (3rd ed. 2002) (citing OFFICE OF TECHNOLOGY ASSESSMENT, THE ELECTRONIC SUPERVISOR 25 (1987)).

system will record every detail, however, distorts the nature of the employer's objective and the reality of the threat.

¶24 Employers seek to maximize productivity, but they must do so with an understanding that they are dealing with employees who are limited by their own human nature. Even the finest employee may be guilty of the occasional *ESPN.com* break and this deviation is perfectly acceptable so long as that employee is productive relative to his peers.⁶² An employer is aware that a *Google* search for a doctor is entirely that employee's own business and that permitting employer resources to be used to that end will likely increase productivity by saving time. With regards to those occasions where an employee speaks out against management to a third person, many times employers will respect co-worker communications so long as they do not disrupt the work environment. In those cases where an employer does take action against the employee it is often justified, as employers should not be required to tolerate subversive commentary that achieves no constructive purpose. Furthermore, being caught chatting about inappropriate topics over email is almost indefensible if notice of monitoring has been provided.

¶25 Along the same lines, an employer's ability to monitor often must be balanced with considerations of employee morale and job satisfaction. For example, one University of Wisconsin study found that workers whose communications were monitored suffered from higher rates of depression, anxiety and fatigue than those not subject to monitoring at the same business.⁶³ It is logical to assume that excessive monitoring aggravates these symptoms. Ultimately, if an employer fails to determine the appropriate bounds of propriety, her business will suffer regardless of whether electronic privacy is granted employees or not.

¶26 Examples such as the chair device that monitors wiggling and the public bathroom log also demonstrate that monitoring abuses, when they occur, are not limited to computer surveillance. An employer may abuse her authority regardless of whether new technology is made available to her or not. If the bargaining power of the employer is that substantial, it is a wonder how an electronic privacy statute will improve the workplace, given the fact that excessive monitoring can take so many different forms. Employers who are not permitted to monitor computer activity by using a software program may eliminate individual office space, or require employees to create individual logs and print out all correspondence. As

⁶² See Atwell, *supra* note 59, at 96 ("Management needs only a ranking of its employees in terms of productivity for purposes of promotion, sanctions, or firings").

⁶³ See Peter Blackman & Barbara Franklin, *Blocking Big Brother; Proposed Law Limits Employers' Right to Snoop*, N.Y. L. J., (Aug. 19, 1993), at 5.

noted in one journal of sociology: “Management has long had the tools necessary to tell who was, in its opinion, a good worker and who a bad worker, via observation, auditing and related forms of surveillance of clerical workers.”⁶⁴ The mere fact that some work environments will exist where employer monitoring rights will be abused fails to justify additional statutory protections.

¶27 Even if the employer happens across private information in her monitoring of an employee’s Internet use, several legal principles require that the information be handled with the respect it deserves. The cause of action for public disclosure of private facts forbids the “unreasonable publicity of private information.”⁶⁵ A cause of action under the doctrine of false light arises where “offensive publicity attributes to the plaintiff’s characteristics, conduct, or beliefs that are false, such that the plaintiff is placed before the public in a false position.”⁶⁶ Similarly, defamation prevents false elaboration upon the discrete facts obtained by the employer in the course of his surveillance.⁶⁷ An action for intentional infliction of emotional distress may also lie in those instances that are particularly outrageous.⁶⁸ Additional causes of action may arise depending upon the circumstances or the particular nature of the information.⁶⁹

¶28 Consequently, despite those anecdotal cases where employers have abused their dominant position, most employers do not have an incentive to use electronic monitoring unfairly. Employers will, in most cases, account for the personal lives of their employees, and numerous legal doctrines prevent the misuse of private information obtained by monitoring. Despite these incentives, there will exist those work environments that are substandard to the point of being abusive; there will be those organizations where employees are limited in their ability to voice their disapproval by quitting because job opportunities are limited. Nevertheless, these workplace environments are unlikely to be improved significantly by the creation of additional statutory protections for electronic privacy. Excessive monitoring can take many controlling forms without the aid of computer surveillance if that is the intent of the employer. Still, these instances are exceptions.

⁶⁴ Atwell, *supra* note 59, at 96.

⁶⁵ Gabel and Mansfield, *supra* note 10, at 314.

⁶⁶ *Id.* at 315.

⁶⁷ *See id.* at 317—18.

⁶⁸ *See id.* at 318—19.

⁶⁹ For example, the Fair Credit Reporting Act may govern the use of certain information. 15 U.S.C. §§ 1681, et seq. (2000).

CONCLUSION

¶29 Commentators have attacked the current state of employment privacy law as anachronistic, outmoded and unrealistic, given the new power that computer surveillance software has provided to employers. Other common law countries like the United Kingdom and Australia have responded to these criticisms and set out statutory schemes specifically governing monitoring of employee computer use.⁷⁰ Additional statutory protection in the United States, however, is unnecessary.

¶30 Undoubtedly, U.S. law affords employees little protection against employer monitoring of their Internet activities. As a matter of judicial precedent, this allocation of rights is unlikely to change. With time, as more and more employers realize the need to monitor the Internet activities of their employees and employment decisions are increasingly supported by computer monitoring, fewer employees will believe that their online conversations are confidential.⁷¹ Thus to some extent, the lack of judicial enthusiasm for the privacy of employee Internet activity will render it a public activity.

¶31 This outcome, however, is entirely fair given the nature and purpose of the workplace and the substantial liability employers face for the actions of their employees. Moreover, employers are unlikely to misuse their monitoring privilege as it is in their best interest to balance surveillance needs with employee quality of life, and because employer misuse of personal information is prohibited by a variety of existing legal doctrines. Fundamentally, the Internet has not changed the balance of power in the workplace. Employees have a new and creative way to shirk their responsibilities, and employers have technological means by which they can mitigate these indiscretions.

⁷⁰ See Muckle, *supra* note 5 (discussing UK law); Privacy Amendment (Private Sector) Act of 2000, *supra* note 5 (revising Australian privacy law).

⁷¹ See, e.g., Andrew Bibby, *Electronic Monitoring in the Workplace*, FREELANCER.DK, at <http://www.freelancer.dk/default.asp?pageToLoad=visNyhed%2Easp%3FartikelID%3D248> (last visited Apr. 23, 2004) (noting that a survey revealed that at 215 UK companies, 65 employees had been terminated for inappropriate Internet use); Mulchandani, *supra* note 56 (discussing how an employee can protect herself against workplace monitoring).