Kentucky Law Journal

Volume 96 | Issue 4 Article 5

2008

You Are Being Watched: The Need for Notice in Employer Electronic Monitoring

Mindy C. Calisti
University of Kentucky

NOTES

You Are Being Watched: The Need for Notice in Employer Electronic Monitoring

Mindy C. Calisti[1]

INTRODUCTION

LIVING in present-day society, it is impossible to avoid the fact that we are being watched—*everywhere*. In the past year, we have been bombarded with news stories about employers eavesdropping on the phone calls and e-mails of the public relations department[2], astronaut Lisa Nowak's discovery of racy e-mails between her love interest and romantic rival[3], newspaper headlines cautioning *Web Surfers Beware: The Boss Is Watching*,[4] and the ever-present electronic recordings notifying us that our phone calls are being "monitored for quality assurance purposes." Perhaps it is the product of maturing in a technologically driven society, but third party monitoring has become a customary practice in certain contexts. Why then is employer monitoring of employee Internet and e-mail usage such a controversial subject in society and the law? For the majority of employees, the concern with employer monitoring may have nothing to do with the employee's *reasonable expectation of privacy* in the workplace, but result instead from an *expectation of notice* when being monitored.

This expectation of notice, however incorrect the assumption may be, is being perpetuated in the employee privacy context. An ABC News segment featuring interviews of employees from varied occupations

1 B.A. Art History, 2005, University of Kentucky; J.D. expected 2008, University of Kentucky College of Law. The author would first and foremost like to thank her family for their support and encouragement throughout her legal education. The author would also like to thank Jill Fraley for reading an early draft of this Note and for her friendship over these past three years.

2 Molly Selvin & Abigail Goldman, *Watching workers: a delicate balance; Policies on monitoring staff haven't kept up with technology, raising the risk of missteps*, L.A. TIMES, Mar. 10, 2007, at C1.

3 Siri Agrell, *Astronaut saw spicy e-mails sent from space; Reading ex-boyfriend's raunchy missives may have launched Nowak's odd mission*, THE GLOBE AND MAIL, Mar. 7, 2007, at A3.

4 Diane Stafford, *Web Surfers Beware: The Boss Is Watching*, PITT. POST-GAZETTE, Mar. 4, 2007, at J-1.

addressed an employer's right to access its employees' communications.[5] One of the featured employees commented that he has:

> been of the opinion that because it's company property, both the programs and the hardware, they should be able . . . to look at [e-mails and Internet usage] . . . [Accordingly, there isn't necessarily] an expectation of privacy at work, so long as . . . the company . . . makes it known . . . that in fact . . . they have monitoring processes in place.[6]

In addition, many employment publications strongly recommend that employers offer notice when they begin monitoring their employees.[7] However, despite these views, per federal statute, employers are not required to provide any form of notice.[8]

Although requiring notice when monitoring appears reasonable, only two states, Delaware and Connecticut, currently mandate that employees be notified of computer monitoring.[9] While a recent study from the American Management Association ("AMA") suggests that 80% of those surveyed do inform their employees of monitoring,[10] the AMA's concept of what qualifies as notice is highly insufficient. Many employers "notify" employees through either their new hire orientation materials or the Intranet. As this "notice" will not reach a large portion of the employee population, there is a great need for a federal statute to provide uniform guidelines on employer monitoring and notice.

With 76% of employers monitoring their employees' Web activity,[11] it is safe to assume that most employers, large and small, are watching electronic activity. Despite this startling figure, the United States is noticeably lagging in federal legislation to regulate an employer's right to monitor and to provide remedies if the employer surpasses those rights. This Note argues that the United States must enact standardized notice procedures so that employers have clear guidance on their ability to monitor and employees can be clearly informed about the scope and timing of the monitoring. Part I addresses an employee's privacy rights in the workplace by discussing the Fourth Amendment's reasonable expectation of privacy standard, America's property rights rationale and the development of workplace monitoring

---

5 *ABC News: Big Brother at Work; Office Spying* (ABC television broadcast Dec. 5, 2006).

6 *Id.*

7 Lisa J. Sotto & Elisabeth M. McCarthy, *An Employer's Guide to US Workplace Privacy Issues*, THE COMPUTER & INTERNET LAWYER, Jan. 2007, at 1. According to the authors, employers should "clearly inform employees on the full scope of monitoring in an employee handbook or e-mail to all employees." *Id.*

8 *See infra* notes 53–65 and accompanying text.

9 *See* CONN. GEN. STAT. § 31–48d (2006); DEL. CODE ANN. tit. 19, § 705(b) (2006).

10 AMA/EPOLICY INSTITUTE RESEARCH, 2005 ELECTRONIC MONITORING & SURVEILLANCE SURVEY 1, www.amanet.org/research/pdfs/EMS_summary05.pdf.

11 *Id.*

practices and case law.[12] Part II considers the current remedies available for employees who have been harmed by their employers monitoring.[13] This section argues that the current state of federal law leaves employees with virtually no remedy when there has been a violation of privacy. Part III presents an argument for the necessity of notice and includes insight on two unsuccessful federal bills, the Delaware and Connecticut statutes, and the European approach to notice and their employer's monitoring.[14] This section will provide guidance on the best methods of developing and structuring the necessary notification guidelines. While notice may not be the ultimate answer for the loss of privacy in the face of new technology, it will provide a workable temporary solution to address the glaring deficiencies in the current federal privacy legislation.

I. EMPLOYEE PRIVACY IN THE WORKPLACE

When determining whether an employee's privacy rights have been violated, it ultimately becomes necessary to establish that the employee's expectation of privacy was reasonable. The reasonable expectation of privacy had its origin in *Katz v. United States*.[15] Quoting Harlan's concurrence in *Katz*, the court in *Smith v. Maryland*[16] established a two–part test for determining whether an individual has a reasonable expectation of privacy. A reasonable expectation of privacy is conditioned upon: (1) an "actual (subjective) expectation of privacy" and (2) an expectation "that society is prepared to recognized as reasonable,"[17] or "'justifiable under the circumstances."[18] The reasonable expectation of privacy standard and the accompanying two–part test arose in the context of Fourth Amendment violations. Although a Fourth Amendment violation only occurs when a state actor[19] (which includes public employers) conducts an unreasonable search and seizure, the standard is relevant to understanding private employee expectations of privacy and their accompanying cultural and social justifications.

It is particularly appropriate to examine Fourth Amendment search and seizure cases that involve the workplace. In the cases that involve

12 *See infra* notes 15–52 and accompanying text.

13 *See infra* notes 53–72 and accompanying text.

14 *See infra* notes 73–125 and accompanying text.

15 Katz v. U.S., 389 U.S. 347, 353 (1967) (Harlan, J., concurring).

16 Smith v. Maryland, 442 U.S. 735, 740 (1979).

17 *Id.* (quoting *Katz*, 389 U.S. at 361).

18 *Id.* (quoting *Katz*, 389 U.S. at 353).

19 Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085, 1150 (2002) ("[T]he federal constitution is firmly entrenched in the concept that constitutional rights apply only against state actors"). *See also* Shawn C. Helms, *Translating Privacy Values with Technology*, 7 B.U. J. SCI. & TECH. L. 288, 314 (2001).

an employee's claim on a Fourth Amendment (or the state constitution equivalent) violation, there are generally two distinct lines of analysis. Many state courts have applied the *Smith v. Maryland* standard requiring that employees demonstrate both prongs in the analysis.[20] A minority of states have held that public employees have no reasonable expectation of privacy at work because they lack a possessory interest in the workplace.[21]

Continuing the long-standing majority analysis of a limited expectation of privacy when the employee has notice,[22] a Ninth Circuit case from 2007 provides insight into the type of notice that will trigger this lesser expectation. In *United States v. Ziegler*,[23] the defendant was charged with receipt of obscene materials for viewing child pornography Web sites while at work. Filing a motion to suppress the evidence, the defendant claimed the computer search, which involved the employer's copying of his hard drive, was in violation of the Fourth Amendment.[24] However, the court held that, although the employee might have a reasonable expectation of privacy in his office, the employer "could give valid consent to a search of the contents of the hard drive of [the defendant's] workplace computer because the computer is the type of workplace property that *remains within the control the employer* 'even if the employee has placed personal items in [it].'"[25]

Additionally, the *Ziegler* court noted that because the employer frequently monitored its employees' Internet activity, and that "upon their hiring . . . employees were apprised of the company's monitoring efforts through training and an employment manual,"[26] the defendant "*could not*

20 In *People v. Rodriguez*, 69 N.Y.2d 159, 162 (N.Y. 1987), the court held that "[a]mong the factors to be considered are whether the individual took precautions to maintain privacy, the manner in which the individual used the premises and whether the individual had the right to exclude others from the premises." *See also* Gatlin v. U.S., 833 A.2d 995, 1005 (D.C. 2003); Cowles v. State, 23 P.3d 1168, 1170 (Alaska 2001); State v. Jimenez, 729 A.2d 693, 696 (R.I. 1999).

21 *See* Hall v. State, 574 S.E.2d 610, 613–14 (Ga. Ct. App. 2002).

22 *See* United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (CIA division's official Internet usage policy eliminated any reasonable expectation of privacy that employee might otherwise have in copied files); Muick v. Glenayre Electronics, 280 F.3d 741, 743 (7th Cir. 2002) (employee had no reasonable expectation of privacy in laptop files where employer announced it could inspect laptops it furnished to employees and employer owned laptops); Wasson v. Sonoma County Junior Coll., 4 F. Supp. 2d 893, 905–06 (N.D. Cal. 1997) (employer's computer policy giving it "the right to access all information stored on [the employer's] computers" defeats employee's reasonable expectation of privacy in files stored on employer's computers).

23 United States v. Ziegler, 474 F.3d 1184 (9th Cir. 2007).

24 *Id.* at 1187.

25 *Id.* at 1191 (quoting O'Connor v. Ortega, 480 U.S. 709, 716 (1987)) (emphasis added).

26 *Id.* at 1192.

reasonably have expected that the computer was his personal property, free from any type of control by his employer."[27]

While this decision will confer some privacy rights to protect employees from unconstitutional searches,[28] it likely will not affect the rights of private employers to control and monitor employee computer use. However, unsure of *Ziegler*'s future applications, more employers may be encouraged to demarcate electronic monitoring guidelines. One commentator noted that, because the court placed significant emphasis on the employer's electronic surveillance guidelines, "an employer who has a policy of monitoring those computers may lawfully access that data and provide it to the government."[29] The company's monitoring policy in *Ziegler*, which included provisions "that the computers were company–owned and not to be used for activities of a personal nature",[30] follows the traditional property rights argument for monitoring and proved successful in significantly reducing the employee's expectation of privacy in the workplace.

A. Property Right Rationale and the Lesser Expectation of Privacy in the Workplace

As *Ziegler* demonstrates, when dealing with electronic surveillance and the protection of personal information, American courts generally employ a property rights approach, which explains the perceived lesser expectation of privacy in the workplace.[31] This approach holds that because "employers own the work tools, they can initiate surveillance at will."[32] The rationales for this approach are two–fold: (1) "Employees have no reasonable expectation of privacy when using company e–mail/Internet facilities;" and (2) "The employer's ownership of these work tools entitle [it] to monitor their use in any way [it] deems fit."[33] Under this rationale, most American employers have virtually no limits on their ability to monitor their employees e–mail and Internet usage. Thus, "American employers have what is in effect an absolute immunity from constitutional, common law, and federal statutory remedies for abusive surveillance practices, with few exceptions."[34] This

27 *Id.* (emphasis added).

28 *Id.* at 1189. The court found that "employees retain at least some expectation of privacy in their offices." *Id.*

29 Mintz Levin Employment, Labor and Benefits Group, *United States: Ninth Circuit Reaffirms Need For Employers To Establish and Communicate Electronic Monitoring Policies*, MONDAQ BUS. BRIEFING, Feb. 7, 2007.

30 *Ziegler*, 474 F.3d at 1192.

31 Karen Eltis, *The Emerging Approach to E–Mail Privacy in the Workplace: Its Influence on Developing Caselaw in Canada and Israel: Should Others Follow Suit?*, 24 COMP. LAB. L. & POL'Y J. 487, 499 (2003).

32 *Id.*

33 *Id.* at 498.

34 Michael L. Rustad & Sandra R. Paulsson, *Monitoring Employee E–Mail and Internet*

statement essentially means that most employee claims of a workplace privacy violation will be decided in favor of the employer.

In addition to not recognizing a reasonable expectation of privacy, some courts assume that the employer will engage in monitoring. According to the Seventh Circuit, in *Muick v. Glenayre Electronics*:

> The laptops were [the employer's] property and it could attach whatever conditions to their use it wanted to. They didn't have to be reasonable conditions; but the abuse of access to workplace computers is so common (workers being prone to use them as medium of gossip, titillation, and other entertainment and distraction) that reserving a right of inspection is so far from being unreasonable that failure to do so might well be thought irresponsible.[35]

Indeed, in the co–worker harassment context, it may be irresponsible for the employer not to engage in monitoring. The United States Supreme Court has held that "an employer can be liable where its own negligence is a cause of the harassment. An employer is negligent with respect to sexual harassment if it knew of or should have known about the conduct and failed to stop it."[36] In this situation, an employer who is aware of the harassment but fails to investigate (i.e., monitor) may be found negligent.[37]

With the property rights rationale, employers are not only given the authority, but are also seemingly encouraged to monitor simply because they own the computer. This conclusion is supported by the Government's successful position against the alleged violation of the reasonable expectation of privacy with a workplace computer in *United States v. Ziegler*.[38] In their brief, the Government argued:

> Society could not deem objectively reasonable that privacy interest where an employee uses a computer paid for by the company; Internet access paid for by the company, in the company office where the company pays the rent .... This is certainly even more so true where the company has installed a firewall and a whole department of people whose job it was to monitor their employee's Internet activity.[39]

Since the employer owned the computer in issue, the employee had no reasonable expectation of privacy. The employer had the authority to monitor in any way it deemed necessary.

Usage: Avoiding the Omniscient Electronic Sweatshop: Insights from Europe, 7 U. PA. J. LAB. & EMP. L. 829, 896 (Summer 2005).

35 Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002).

36 Burlington Indus. v. Ellerth, 524 U.S. 742, 759 (1998).

37 *See id.* at 758.

38 United States v. Ziegler, 474 F.3d 1184 (9th Cir. 2007).

39 *Ziegler*, 474 F.3d at 1188–89.

B. Workplace Investigations

1. *Internet Usage and E-mail Monitoring.*—In addition to the property rights argument, there are several other reasons posited for the appropriateness of employer monitoring, namely:

> [1] preventing the misuse of bandwidth as well as the loss of employee efficiency when employees surf the Internet; [2] ensuring that the company's networking policies are being implemented; [3] preventing lawsuits for discrimination, harassment or other online torts; [4] preventing the unauthorized transfer of intellectual property and avoiding liability due to employees making illegal copies of copyrighted materials; [5] safeguarding company records which must be kept to comply with federal statutes; [6] deterring the unlawful appropriation of personal information, and potential spam or viruses; and [7] protecting company assets including intellectual property and business plans.[40]

Whatever reasoning the employer uses, case law has established that employers are permitted to investigate suspected employee misconduct.

Many companies first began to monitor their employees e-mail or Internet usage in the early to mid-1990s at a time when very few had formal monitoring policies in place.[41] Despite the lack of policies, "[c]ourts were surprisingly receptive to employers' arguments that the employees had no reasonable expectation of privacy in workplaces, even where the company gave the employees no warning that they would be intercepting electronic communications."[42] These courts viewed electronic monitoring as an acceptable and necessary employer practice.[43]

In one of the earliest employer monitoring cases, *Smyth v. Pillsbury Co.*, the court found no "reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management."[44] In the case, an employee was fired for voluntarily transmitting "inappropriate and unprofessional comments" over the employer's e-mail system.[45] Despite the employer's assurances that his e-mails would remain confidential, the court found no reasonable expectation of privacy because the correspondence had been communicated over the company's system. The court held that liability would attach only when the "intrusion is substantial and would be

40 Rustad & Paulsson, *supra* note 34, at 836.

41 *Id.* at 854.

42 *Id.*

43 *Id.*

44 Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996).

45 *Id.* at 98–99.

highly offensive to the 'ordinary reasonable person,'"[46] which was not the situation in this case. Thus, the employee's claim of wrongful termination in violation of "public policy which precludes an employer from terminating an employee in violation of the employee's right to privacy" [47] failed since the employee had no expectation of privacy in the employer's e-mail system.[48]

Adopting reasoning similar to *Smyth*, the court in *McLaren v. Microsoft Corp.* held that there was no reasonable expectation of privacy when the employer accessed personal folders on his office computer and then released that information to third parties.[49] According to the court, the e-mails were not the employee's personal property, but were rather a part of the office environment.[50] Therefore, even if the employee did have an expectation of privacy with regard to those e-mail messages, "the company's interest in preventing inappropriate and unprofessional comments, or even illegal activity, over its e-mail system would outweigh [the employee's] claimed privacy interest in those communications."[51]

Although they never received notice of the monitoring, the employees in the aforementioned cases were determined to have an *unreasonable* expectation of privacy by courts utilizing the property-based rationale. In addition to this employer ownership argument, courts have noted additional justifications for the employer monitoring: the technological resources are provided to employees for business activity uses and the monitoring enhances productivity while preventing fraud and theft.[52] The numerous acceptable rationales for surveillance and the limited number of private sector employer monitoring cases coupled with the limited remedies available for employees result in a high probability that the employee will be unsuccessful in their suit. However, one significant way to hold employers more accountable is to require that they provide notification to employees before monitoring, and to provide sufficient remedies when the employers fail to comply.

---

46 *Id.* at 100 (quoting Borse v. Piece Goods Shop, Inc., 963 F.2d 611, 621 (3d Cir. 1992)). According to the court, "in determining whether an alleged invasion of privacy is substantial and highly offensive to a reasonable person, the Court of Appeals predicted that Pennsylvania would adopt a balancing test which balances the employee's privacy interest against the employer's interest in maintaining a drug-free workplace." *Id.*

47 *Id.* at 100.

48 *Id.* at 101.

49 McLaren v. Microsoft Corp., No. 05-97-00824, 1999 WL 339015 (Tex. App. May 28, 1999).

50 *Id.* at *4.

51 *Id.* at *5.

52 *See, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97, 100 (E.D. Pa. 1996); *McLaren*, 1999 WL 339015, at *5; Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996).

II. CURRENT "REMEDIES" FOR EMPLOYEES

American employees in the private sector have no constitutional remedy against employer monitoring, even when implemented in a discriminatory fashion and without notice.[53] Thus, a private sector employee must look elsewhere if he believes the employer's monitoring violated his reasonable expectation of privacy. Unfortunately for the private employee, "the current state of the law is that private employees have no constitutional, federal statutory, or common law remedies to redress employer abuses of e–mail or Internet monitoring."[54] Thus, without a change in the law, many employee privacy suits will be unsuccessful.

A. The Electronic Communications Privacy Act of 1986

The most fundamental protection for the privacy of electronic communications is found in the Electronic Communication Privacy Act ("ECPA").[55] Employees disciplined or fired because of their e–mail or Internet usage typically include a claim seeking redress under the ECPA. According to the "Title I" of the federal statute, it is unlawful for any person to "intentionally intercept[s], endeavor to intercept, or procure[s] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[56] Under "Title II," it is a federal crime if a person "intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication . . . ."[57]

Although the language of Title I and II technically covers private employers, employee monitoring is not significantly limited by the ECPA. Several statutory exceptions or defenses come to the employer's rescue. Title I contains exceptions for "business use in the ordinary course of business," "providers of communication systems," and "consent."[58] Likewise, Title II covers exceptions for "providers of communications" and "authorization by users of communications systems."[59] In addition to

53 Rustad & Paulsson, *supra* note 34, at 841.

54 *Id.* at 843.

55 Gail Lasprogata, Nancy J. King & Sukanya Pillay, *Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy Through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada*, 2004 STAN. TECH. L. REV. 1, 72 (2004).

56 The Wiretap Act, 18 U.S.C. § 2511 (1986).

57 The Stored Communications Act, 18 U.S.C. § 2701 (1986).

58 Jay P. Kesan, *Cyber–Working or Cyber–Shrinking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 296 (2002).

59 Lasprogata et al., *supra* note 55, at 73.

the statutory exceptions, the majority of cases under the Act have held that the "interception of e-mails must occur contemporaneously with their transmission to violate the ECPA. Based on this interpretation of 'intercept,' an employer who retrieves e-mail from an employee's mailbox *following* the transmission of the e-mail has not violated the Wiretap Act."[60] If an employer meets one of the exceptions or defenses, the EPCA does not place any restrictions on the monitoring, and it does not require employee notification of the monitoring. According to one commentator on the matter, in light of the "breadth of the exceptions under the EPCA and the ability of companies to adopt comprehensive electronic communications policies, it will be difficult for employees to sue their employers under the EPCA for electronic monitoring in the workplace."[61]

A recent case helps illustrate the pro-employer exceptions which make an employee's EPCA claim all but impossible. In *Fraser v. Nationwide Mutual Insurance Co.*,[62] the employer, fearing that an employee might have been disseminating confidential information to a competitor, searched the employee's e-mails that were stored on the company's server. Once his employment was terminated, the employee brought an action against the employer, including damages claims under both Titles I and II of the ECPA. The Third Circuit rejected the employee's claims, holding that "an 'intercept' under the ECPA must occur contemporaneously with transmission."[63] Since the employer read the messages while they were in storage, the court ruled that they did not "intercept" the e-mails within the meaning of the ECPA.[64] Since most employers' behavior in electronic surveillance will be similar to Nationwide's, it will be unlikely that an employer's monitoring would violate the "interception" provision. As long as the employers' meet one of the vast exceptions, most commonly by being the provider of the workplace e-mail system, "they may access employees' stored e-mail messages (regardless of the originator's designation of them as personal or professional) and are exempt from liability under the ECPA."[65]

B. Common Law Privacy Rights

The ECPA never indicated that it was preempting other remedies for privacy protection. Thus, employees technically may have other remedies under the common law for invasive employer monitoring. Most attempts by the employees to assert an invasion of privacy claim, however, have

60 Matthew E. Swaya & Stacey R. Eisenstein, *Emerging Technology in the Workplace*, 21 LAB. LAW. 1, 11 (2005).

61 Lasprogata et al., *supra* note 55, at 74.

62 Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107 (3d Cir. 2003).

63 *Id.* at 113.

64 Swaya & Eisenstein, *supra* note 60, at 12.

65 18 TRACY BISHOP HOLTON, CAUSES OF ACTION (SECOND SERIES) § 87 (2006).

returned in favor of the employer.[66] Similar to actions brought under the ECPA, private employee common law privacy claims have tended to be futile.

In the employment context, the most common privacy claim is intrusion of seclusion which requires the employee to establish that "he had a reasonable expectation of privacy and that the employer's review of the private information would be highly offensive to a reasonable person."[67] There is technically a third element, the intrusion, but it is generally a non–issue as courts accept the electronic monitoring as sufficient to establish the requirement.[68] When dealing with these types of claims, "courts will first define the scope of an employee's reasonable expectation of privacy and then balance the employer's business interest against the employee's individual rights. Courts [then] treat the workplace environment, the reason for the intrusion, and the means employed as factors to be considered."[69] The employer can establish the employee's anticipated reasonable expectation of privacy by communicating their electronic monitoring policy to their employees; furthermore, it should be relatively easy for the employer to provide legitimate business reasons for the monitoring.[70] It is argued that employers can insulate themselves from common law privacy liability by notifying employees of their electronic monitoring program.[71] However, courts have been receptive to arguments that employees have no reasonable expectation of privacy, even when the employer gave no notice of their monitoring.[72]

III. Workplace Monitoring and Notice in the United States and Abroad

A. Why Notice?

Given the pro–employer stance of most American courts, notice of the surveillance should be mandatory. This notice will afford protection to both employees and employers once electronic monitoring occurs. Notice significantly decreases the employee's reasonable expectation of privacy, and thus helps further insulate the employer from liability. Further, it can establish the e–mail and Internet activity deemed inappropriate, and will give employees a better understanding of the conduct that would violate the employment policies. Notice can additionally have a deterrence effect—it

66 Janet G. Payton, Corporate Counsel's Guide to Privacy, § 7:6 (2006).

67 Kesan, *supra* note 58, at 302.

68 *Id.*

69 *Id.* at 303.

70 *Id.*

71 *Id.* at 304.

72 Rustad & Paulsson, *supra* note 34, at 854.

might deter some employers from engaging in unlawful monitoring, and it would certainly deter many employees from engaging in conduct that could be grounds for termination. The examples discussed below, including two failed federal statutes, current state statutes, and the laws of Europe should provide a working framework for future federal legislation which is decidedly needed in the United States.

B. The Proposed Privacy for Consumers and Workers Act

In the early 1990s, several bills appeared in Congress that intended to deal with the noticeable gaps of the ECPA.[73] One such bill, the Privacy for Consumers and Workers Act ("PWCA"), attempted to constrain the exceptions businesses were granted by the ECPA.[74] The proposed statute's language indicated that it intended to "prohibit the collection, storage, analysis or reporting of information concerning an employee's activities by means of... electronic observation and supervision... which is conducted by any method other than direct observation by another person."[75] Further, the PCWA would have provided the employee with the "right to know" the details of the monitoring, namely, where and when the monitoring would occur and how the employer planned to use the evidence.[76] The employer would also have been required to notify the employee once the surveillance actually occurred and this notification could be accomplished through a signal light, beeping tone, verbal warning or other system.[77] With its numerous constraints on the employer and the failure to account for different business monitoring needs, the ambitious bill did not survive.[78] However, the PCWA is useful in that it provides some guidance as to the form and content of notice that the drafters and critics found reasonable.

C. The Proposed Notice of Electronic Monitoring Act

Nearly a decade after PWCA failed to pass, Congress introduced the Notice of Electronic Monitoring Act ("NEMA") in 2000. Although NEMA intended to enhance employee privacy rights, this proposed bill did not put any restrictions on monitoring; rather it required notice at specified times throughout the employee's tenure.[79] "NEMA acknowledges that, while

---

73 Kesan, *supra* note 58, at 299.

74 *Id.*

75 Jill Yung, *Big Brother is Watching: How Employee Monitoring in 2004 Brought Orwell's 1984 to Life and What the Law Should Do About It*, 36 SETON HALL L. REV. 163, 205 (2005).

76 Lee Nolan Jacobs, *Is What's Yours Really Mine?:* Shmueli v. Corcoran Group *and Penumbral Property Rights*, 14 J.L. & POL'Y 837, 863 (2006).

77 *Id.*

78 Yung, *supra* note 75, at 206.

79 William R. Corbett, *The Need for a Revitalized Common Law of the Workplace*, 69 BROOK.

employees should not have an expectation of privacy in e-mail voluntarily sent, stored, or received on the company's system, the employees are entitled to clear notice from employers who choose to exercise their monitoring rights."[80] This rationale made it much less ambitious and more focused than its predecessor; however, this did not change its ultimate outcome.

Had it been enacted, NEMA would have required that employers give notice when electronic monitoring would be taking place. Sufficient notice in this context would have required the employer to describe the form of communication that would be monitored, the means by which the monitoring would be accomplished, the kind of information that would be obtained, the frequency of the monitoring, and how the information would be gathered.[81] The bill appeared to find a point of compromise between employers and employees, and during the hearings, testimony by James Dempsey, from the Center of Democracy and Technology, seems to sum up the middle ground: "the bill merely requires employers to tell their employees in advance what types of monitoring they will be subject to. Yet this alone will go a long way to restoring to workers their sense of dignity, which is a large part of the concept of privacy."[82]

NEMA intended to amend section 2711 in Title 18 of the United States Code, and would have read:

> Except as provided in subsection (c), an employer who intentionally, by any electronic means, reads, listens to, or otherwise monitors any wire communication, oral communication of an employee of the employer, or otherwise monitors the computer usage of an employee of the employer, *without first having provided the employee notice* meeting the requirements of subsection (b) shall be liable to the employee for relief as provided in subsection (d).[83]

The timing requirement insisted that the employer give notice at three occasions: before the electronic monitoring occurred, when the employee began his employment, and annually after that.[84]

Despite being hailed as "part of the answer to one of the major concerns of the American public today—the loss of privacy in the face of new technology,"[85] Congress failed to pass NEMA. As is often the case,

---

L. REV. 91, 115 (2003).

80 Meir S. Hornung, Note, *Think Before You Type: A Look at E-mail Privacy in the Workplace*, 11 FORDHAM J. CORP. & FIN. L. 115, 156 (2005).

81 Notice of Electronic Monitoring Act, H.R. 4908, 106th Cong. § 2711(b) (2000).

82 *Electronic Communications Privacy Act of 2000, Digital Privacy Act of 2000 and Notice of Electronic Monitoring Act: Hearing on H.R. 5018, H.R. 4987 and H.R. 4908 Before the House Subcomm. on the Const. of the Comm. on the Judiciary*, 106th Cong. (2000) (statement of James X. Dempsey, Center for Democracy and Technology).

83 H.R. 4908 § 2711(a)(1) (emphasis added).

84 H.R. 4908 § 2711(a)(2).

85 *Notice of Electronic Monitoring Act: Hearing on H.R. 4908 Before the Subcomm. on*

critical concerns outweighed the praise.[86] Congress shelved NEMA in late September of 2000 because of "concerns [expressed] 'by various business and employer coalitions . . . [regarding] the potential for an 'increase in employment litigation . . ."[87] The strongest criticism involved the lack of delineated methods of notice. The employer groups claimed that by merely requiring that "clear and conspicuous notice" be given might give rise to more litigation because the employee could claim his advance notice was neither clear nor conspicuous.[88] In addition, critics claimed NEMA would impose too great a burden on employers. As was duly noted, however, "if a company has the resources to engage in employee monitoring, it should have the resources to issue notices to each employee."[89] The failure of both the PCWA and NEMA does not paint an optimistic picture for future efforts for electronic monitoring legislation. However, these unsuccessful statutes as well as the state laws mentioned below provide guidelines for future efforts of federal legislation.

D. State Laws Requiring Notice

Very few states regulate employers' monitoring of e-mail and Internet activity. However, the statutes and case law discussed below provide guidance as to both the content and frequency of notice that can and should be provided to employees before electronic surveillance is conducted. Most state laws mirror Title III of the EPCA "and therefore similarly do not prohibit employer monitoring of e-mail."[90] However, both Delaware and Connecticut modeled their statute after NEMA, and therefore give employees greater protection and remedies against employer surveillance conducted without prior notice.

1. *Connecticut and Delaware.*—Clearly evoking the language of NEMA, Connecticut General Statute section 31–48d provides that "each employer who engages in any type of electronic monitoring shall give *prior written notice* to all employees who may be affected, informing them of the types

---

the Constitution of the H. Comm. on the Judiciary, 106th Cong. (2000) (testimony of James X. Dempsey, Center for Democracy and Technology).

86 Yung, *supra* note 75, at 208. One such critic Marc Rotenberg, Executive Director of the Electronic Privacy Information Center, "accused the law of being counterproductive for employees, whose reasonable expectation of privacy would be undermined by an employer's provision of notice." *Id.*

87 *Id.*

88 Nathan Watson, Note, *The Private Workplace and the Proposed "Notice of Electronic Monitoring Act:" Is "Notice" Enough?*, 54 FED. COMM. L.J. 79, 97 (2001).

89 *Id.* at 98.

90 Victor Schachter, *Privacy in the Workplace*, *in* SIXTH ANNUAL INSTITUTE ON PRIVACY LAW: DATA PROTECTION—THE CONVERGENCE OF PRIVACY AND SECURITY 153, 209 (Practicing Law Institute 2005).

of monitoring which may occur."[91] According to the statutory language, every employer, regardless of their size must post "in a conspicuous place . . . [written] notice concerning the types of electronic monitoring which the employer may engage in."[92] This type of posting will be enough to constitute prior written notice, and an employee's continued use of employer-provided equipment after the notification may indicate consent to monitoring.[93]

Strikingly similar to the Connecticut statute, Delaware requires that prior notice be given to employees before an employer may monitor e-mails or Internet usage.[94] Originally, however, the statute only required that notice be given once and that it be signed by the employee.[95] The statute was amended to its current form in 2002, and is now much more protective of the employee's workplace privacy rights. The most significant change to section 705(b) was, " (1)[Employer must] *[p]rovide[s] an electronic notice of such monitoring* or intercepting policies or activities to the employee *at least once during each day the employee accesses* the employer-provided e-mail or Internet access services; or (2) *Has first given a 1-time notice to the employee of such monitoring or intercepting activity or policies.*"[96] According to the statute then, the notice must either be provided on a daily basis or be acknowledged by employee. If notice takes the form of (2), it is not required to be in writing; instead, notice can also take the form of an electronic record or any other electronic form that the employee acknowledges either in writing or electronically.[97]

2. *California.*—Unlike Connecticut and Delaware, California does not have a statute regulating notice and monitoring. Despite the absence of state legislation, California courts have held that "employees do not have a reasonable expectation of privacy in their e-mail messages, *provided they are given adequate notice of monitoring and searching.*"[98] The court in *Bourke v. Nissan Motor Corp.* held that the employee had no reasonable expectation of privacy because forms signed by employees advised them that company

91 CONN. GEN. STAT. § 31-48d (b) (1) (2006) (emphasis added).

92 *Id.*

93 Ira David, *Privacy Concerns Regarding the Monitoring of Instant Messaging in the Workplace: Is it Big Brother or Just Business?*, 5 NEV. L.J. 319, 331 (2004).

94 1 L. CAMILLE HEBERT, EMPL. PRIVACY LAW § 8A:22 (2006).

95 *Id.*

96 DEL. CODE ANN. tit. 19, § 705(b) (2006) (emphasis added).

97 *Id.*

98 Victor Schachter & Shawna M. Swanson, *Workplace Privacy and Monitoring: New Developments Affecting the Rights of Employers and Employees*, *in* SEVENTH ANNUAL INSTITUTE ON PRIVACY LAW: EVOLVING LAWS AND PRACTICES IN A SECURITY-DRIVEN WORLD 135, 149 (Practicing Law Institute 2006) (emphasis added).

computers were to be used for "business purposes only.[99] In light of the employee's signature on the "Computer Use Registration Policy" and their knowledge that random e-mails were reviewed to ensure compliance, the court rejected the employee's invasion of privacy claims.[100]

In addition to the relevant court decisions, California proposed an electronic monitoring bill during the 2003–2004 session. Had it passed, this bill would have required employers to provide notice to employees of their intent to monitor and collect information about their electronic activities.[101] The law was intended to be a notice statute—"employers would have simply been required to provide a warning that specified the activities, including those not related to the employer's business, that would be monitored and a description of the information sought through this process."[102] Despite passing in both houses, the bill was vetoed by Governor Schwarzenegger.[103]

E. Notice and Employee Monitoring in Europe

Unlike America's property rights regime, European countries operate under a human rights model when addressing employee privacy rights. While these countries recognize that employers have legitimate interests in ensuring the productivity of their businesses and protecting themselves against liability by their employees, the European Union has made it clear that, with regard to employee privacy in the workplace, the employee's human dignity trumps the other considerations.[104] As a result, "European employers . . . are required to give employees clear and conspicuous note about notice. If actual notice of surveillance is not established, any interception of electronic communications is considered to be unlawful."[105]

In addition to utilizing the human rights rationale, the European Commission adopted a Directive on Privacy and Electronic Communication in 2002.[106] The directive states that "the confidentiality of communications prohibits the practice of interception or surveillance of private communications between others over networks . . . . Gaining access

99 Bourke v. Nissan Motor Corp, No. B068, 705 Cal. App. 2d (July 26, 1993) (unpublished opinion), *available at* http://www.loundy.com/CASES/Bourke_v_Nissan.html.

100 *Id.*

101 Yung, *supra* note 75, at 209.

102 *Id.* at 210.

103 *Id.*

104 Lasprogata et al., *supra* note 55, at 24.

105 Rustad & Paulsson, *supra* note 34, at 897.

106 It is important to note that all European Directives are not themselves a law, instead they are "a direction to the member states to enact implementing legislation consistent with its privacy protection obligations." Lasprogata, *supra* note 55, at 50.

to or storing information from a user's terminal . . . is *only allowed if the user is given clear information* about the purpose of any such invisible activity and is offered the right to refuse it."[107] While this directive does not necessarily include internal work e-mails, if the private employees access a public network, they are automatically protected by the directive.[108]

Since there are no European Union regulations or directives which are specifically intended for electronic employee monitoring, the Article 29 Working Party[109] has attempted to fill the void themselves. Issuing the 2001 Working Opinion and the 2002 Working Document, they have established guidelines that identify the acceptable limits on an employer's ability to electronically monitor.[110] According to these documents, "[b]efore employer monitoring activity can be considered lawful and justified, the employer must comply with seven fundamental data protection principles: necessity, finality, transparency, legitimacy, proportionality, data accuracy, and security."[111] Of particular note, the "transparency requirement" mandates that the employer be open and clear about their activities. While not requiring a written policy, "the transparency rule dictates that employers' monitoring practices be *fully and clearly disclosed* to all employees subject to the policy, along with the reasons for the monitoring."[112]

In addition to the abovementioned directives, when a European employer implements an electronic surveillance policy, it "must adhere to the privacy regulations in each member state in which it is subject to enforcement jurisdiction."[113] Discussed below are a few of the member states' legislation and court decisions with particular emphasis on the requirement of notice in the employer monitoring context.

1. *France.*—In France, "[a]n employer's right to monitor and to interfere with an employee's personal affairs is prohibited under the Employment Code unless the interference is in accordance with the purpose and in proportion to the reason of the interference."[114] Even if the exceptions are met, information of a personal nature cannot be collected unless the French employer has "clearly informed his employees about it and the information about the monitoring is easily available."[115]

107 Rustad & Paulsson, *supra* note 34, at 880 (emphasis added).

108 *Id.*

109 An advisory and independent group which is comprised of representatives from all 27 EU Member States.

110 Lasprogata et al., *supra* note 55, at 39.

111 *Id.* at 41.

112 *Id.* at 44 (emphasis added).

113 *Id.* at 51.

114 Rustad & Paulsson, *supra* note 34, at 892.

115 *Id.*

One French case marks the distinct difference in employee privacy between France and the United States. In *Societe Nikon France v. M. Onof*, the court held that the employer had no legal right to intercept an employee's personal e-mails, *even if* the employer is the supplier of the computer and expressly stated that the computers were not for personal uses.[116] The Court of Cassation declared that "it would be a violation of a fundamental freedom, namely the right to privacy and secrecy of correspondence, for an employer to read personal messages sent or received by their employee on a computer belonging to the employer and used by the employee for work."[117] According to the court, the employer has a general right to monitor e-mail or Internet communications only if the employer has complied with the notice requirement and can prove that the employee had actual notice of the employer's monitoring.[118]

2. *England.*—The electronic surveillance of British employees must comply with the country's implementation of the European Directive on Data Protection. The U.K. Data Protection Act (DPA) provides a remedy for the victims of electronic surveillance. "The DPA requires the 'data controller,' the one processing the information, to notify employees about the monitoring system as well as protect the data."[119] There is one exception to the notice requirement—if the purpose of the employer's monitoring is to prevent a specific crime, then surveillance without notification is permitted.[120]

Additionally, the Employment Practices Data Protection Code[121] ("U.K. Code") is intended to give British employers guidance for their compliance with the United Kingdom's Data Protection Act ("DPA"). According to the U.K. Code, employer monitoring is lawful under the DPA so long as the guidelines in the Code are followed. Most specifically, the U.K. Code recommends that the transparency and proportionality principles be followed. "Employers wishing to electronically monitor their employees must notify employees and any other party to the communication that they are being monitored (transparency) and must eliminate the collection of personal information that is 'irrelevant or excessive' to the employment relationship (proportionality)."[122] In addition, the U.K. Code provides

116 *Id.* at 893–94 (emphasis added).

117 Yohei Suda, *Monitoring E-Mail of Employees in the Private Sector: a Comparison Between Western Europe and the United States*, 4 WASH. U. GLOBAL STUD. L. REV. 209, 255 (2005).

118 Rustad & Paulsson, *supra* note 34, at 892.

119 *Id.* at 886.

120 *Id.* at 886–87.

121 UNITED KINGDOM INFORMATION COMMISSIONER, THE EMPLOYMENT PRACTICES DATA PROTECTION CODE: PART 3: MONITORING AT WORK (2003), *available at* http://www.privacydataprotection.co.uk/pdf/employment_ code_of_ practice.pdf.

122 Lasprogata et al., *supra* note 55, at 60.

recommendations to employers utilizing electronic monitoring software, including: "wherever possible avoid opening e-mails, especially ones that clearly show they are private or personal . . . [and] where practicable, ensure that those sending e-mails to workers, as well as workers themselves, are aware of any monitoring and the purpose behind it."[123]

3. *Germany*.—A few recent German cases suggest that their courts also favor employee notice before the employer's electronic surveillance can occur. According to the cases, "German employers may retrieve an employee's personal electronic communications *only if* in furtherance of a valid business interest, the employee has been *given notice*, and the rules governing Internet connection and e-mail use applied by the employer have been agreed to by the employee's elected work council."[124] Additionally, the employee who violates the employer's monitoring policies cannot be terminated without having first received formal notice of his violation. According to the Regional Labor Court of Hessen, a general warning to all employees is insufficient to uphold an employee's termination without first providing a formal warning to the violating employee.[125]

CONCLUSION: RECOMMENDATIONS FOR PROPER NOTICE

As the court in *United States v. Bailey* held, "an employer's notice to an employee that workplace files, Internet use, and e-mail may be monitored undermines the reasonableness of an employee's claim that he or she believed such information was private and not subject to search."[126] Notice of employer monitoring, then, is necessary for the protection of employee privacy and employer surveillance procedures. As has been discussed, if the employer notifies his employees that an electronic monitoring program is in place, the employee's reasonable expectation of privacy in the workplace is decreased significantly.[127] Thus, notice of potential monitoring actually works to the employer's advantage because it virtually ensures the employer's success against an invasion of privacy lawsuit. Furthermore, it helps to remove the stigma that the employer is spying on his employees.

123 James M. Jordan III, *Recent Developments in Workplace Privacy Outside the U.S.*, in SEVENTH ANNUAL INSTITUTE ON PRIVACY LAW: EVOLVING LAWS AND PRACTICES IN A SECURITY-DRIVEN WORLD 231, 277–78 (Practicing Law Institute 2006).

124 Lasprogata et al., supra note 55, at 55 (emphasis added).

125 *Id.*

126 U.S. v. Bailey, 272 F. Supp. 2d 822, 835 (D. Nebraska 2003).

127 *See supra* notes 74–104 and accompanying text; *see also* Garrity v. John Hancock Mut. Life. Ins. Co., No. CIV. A. 00-12143-RWZ, 2002 WL 974676, at *1 (D. Mass. May 7, 2002) (where the court dismissed employees' claims of invasion of privacy based on their employer's reading of their e-mail on the employer's computer system).

The employees would be fully aware that the monitoring is occurring and could therefore alter their conduct appropriately.

One recommendation is to provide both notice and reasoning before an employer engages in electronic monitoring. "Employers gain a valuable measure of protection by providing clear and specific notice to employees of their legitimate business interests and their policies regarding screening, monitoring and investigating employees' conduct."[128] The employer should establish a reasonable and logical connection between their legitimate business interests and the conduct they are attempting to control.[129] To make notice more effective, the United States should require that notice of potential monitoring be clearly and conspicuously placed in several locations, including but not limited to the company's Intranet, any employee manuals and the employee break room. In terms of timing, notice should also be given at the time of hiring and directly before any monitoring is to occur. This will ensure that the employee actually had a limited reasonable expectation of privacy. While notice may not be the most effective way to deal with the electronic surveillance issues, it is a reasonable and successful solution in Europe, Delaware and Connecticut. The federal government should follow suit and enact legislation that requires notice; it will provide a good foundation for future discussions and will lessen employee concerns regarding expectations of privacy in the workplace.

128 Schachter, *supra* note 90, at 245.

129 *Id.*