MONITORING EMPLOYEE E-MAIL AND INTERNET USAGE: AVOIDING THE OMNISCIENT ELECTRONIC SWEATSHOP: INSIGHTS FROM EUROPE

Michael L. Rustad† & Sandra R. Paulsson††

I. INTRODUCTION

> A decade ago, compliance with privacy requirements was a relatively simple matter for U.S. companies. Privacy laws were, by and large, extremely limited in scope and affected only narrow categories of businesses. In addition, international data transfers were not critical to many businesses, so there was no need to consider requirements that might be imposed by European or Asian nations. The Internet was just emerging as a consumer technology, and spam was still a type of canned meat.[1]

Something is happening in the U.S. workplace, and it is depriving American workers of their privacy rights and companies of their international competitiveness. Workplace privacy has become a matter of great consequence, particularly because American workers are falling victim to e-mail spying, which is occurring without any protection against such abuse. Electronic monitoring software sales are expected to swell nearly five times from $139 million in 2001 to $662 million by 2006.[2] A 2004 survey of employer monitoring verified that "70% of responding

† Michael L. Rustad, Ph.D, J.D., LL.M is the Thomas F. Lambert Jr. Professor of Law & Co-Director of the Intellectual Property Law Concentration at Suffolk University Law School in Boston, Massachusetts.

†† Sandra R. Paulsson, J.D., LL.M is an attorney at Gevers & Partners, an intellectual property law firm in Diegm-Brussels, Belgium.

1. Lisa J. Sotto & Martin E. Abrams, *Needed: A Master Lock for Data*, RECORDER, Jan. 21, 2005.

2. Robin L. Wakefield, *Computer Monitoring and Surveillance: Balancing Privacy with Security*, 74 CPA J. 52 (July 1, 2004) (quoting an International Data Corporation study).

employers have implemented a written e-mail policy governing use and content, 74% monitor employee outgoing and incoming e-mail, and 60% monitor employee Internet connections."[3] Nearly all computer monitoring software permits workplace surveillance without the employees' knowledge, and current law imposes no duty on the part of employers to notify employees before implementing monitoring software.[4]

Two in three U.S. corporate workplaces have no policy requiring their employees to manifest consent to electronic monitoring or acknowledging their workplace monitoring activities.[5] The pervasive practice of employers monitoring e-mail or Internet usage without notice threatens the fundamental rights of American workers. It is a widespread misconception that "e-mail is as private and confidential as communication via the U.S. Postal Service. . . . [M]ost e-mail, voice-mail and computer systems are in fact anything but private and confidential."[6]

F. Scott Fitzgerald's *The Great Gatsby*[7] has been described as "The Great American Novel," because it is the "quintessential work which captures the mood of the 'Jazz Age.'"[8] The second chapter in Fitzgerald's novel describes an outsized billboard advertising optical services.[9] The billboard sign, with its faceless blue eyes gazing out at the valley of ashes, today would be symbolic of the loss of privacy in the electronic workplace. The omniscient eyes on Dr. Eckleberg's billboard are now locked on workers in the electronic workplace where network administrators indiscriminately copy screen shots in real time, scan data files, read e-mail, analyze keystroke performance, and even overwrite passwords.[10] Electronic surveillance by employers is "the merciless electronic whip that drives the fast pace of today's workplace."[11] Just as the use of e-mail and

---

3. Reginald C. Govan & Freddie Mac, *33rd Annual Institute on Employment Law: Workplace Privacy*, 712 PLI/LIT 245, 251 (2004), *available at* WESTLAW, TP-ALL Library.

4. Privacy Rights Clearinghouse, *Electronic Monitoring: Is There Privacy in the Workplace?*, Fact Sheet #7: Workplace Privacy, Sept. 2002, *at* http://www.privacyrights.org/fs/fs7-work.htm.

5. *Survey: Most Employers Monitor E-mail, Internet Use,* SACRAMENTO BUS. J., Oct. 8, 2003, *available at* http://www.bizjournals.com/sacramento/stories/2003/10/06/daily 20.html.

6. C. Forbes Sargent, III, *Electronic Media and the Workplace: Confidentiality, Privacy and Other Issues*, 41 BOSTON BAR J. 6, 6 (May-June 1997).

7. F. SCOTT FITZGERALD, THE GREAT GATSBY (Simon & Schuster 1995) (1925).

8. Catherine Lavender, *F. Scott Fitzgerald, The Great Gatsby (1925), at* http://www.library.csi.cuny.edu/dept/history/lavender/gatsby.html (last modified June 14, 2001).

9. FITZGERALD, *supra* note 7.

10. David Banisar & Sarah Andrews, *The World of Surveillance Pt. 4: Workplace Privacy*, PRIVACY L. & POL'Y REP. 54 (2000), *at* http://www.worldlii.org/cgi-worldlii/disp.pl/au/journals/PLPR/2000/54.html.

11. Robert G. Boehmer, *Artificial Monitoring and Surveillance of Employees: The*

the Internet is nearly universal, so is the inevitability of an electronic sweatshop where U.S. workers have no privacy.[12]

Part I of this Article makes three points using an extended hypothetical case to demonstrate that America is falling behind its European competitors in protecting the privacy rights of workers in the electronic workplace. The hypothetical is about a multinational corporation's electronic surveillance policies. The U.S.-based company is seeking counsel on how to protect its rights and avoid liabilities in implementing a program to monitor e-mail or Internet usage of its employees located in Europe as well as in the United States.

The first point is that a company's monitoring practices are often justified because of the liabilities created by employees' misuse of e-mail and the Internet. The second point is that employers enjoy what is in effect an absolute immunity against employees' claims that monitoring violates their privacy. The U.S. law of electronic monitoring "accords the employer near plenary power to govern the workplace; in fact, to govern the worker."[13] At present, U.S. employees have no meaningful constitutional, common law, or statutory protection from employer abuse by intrusive e-mail or Internet monitoring. While there may be compelling reasons to monitor e-mail in both the United States and Europe, there is a divergence in the value placed upon informational privacy. The third point is that although European employers monitor their employees' e-mail or Internet usage, they must take reasonable precautions to protect their employees' privacy.

Part II continues with the hypothetical of the multinational company implementing electronic surveillance in its U.S. and European workplaces. The hypothetical confirms that the U.S. is lagging behind Europe in balancing workplace monitoring against the privacy rights of employees.[14] This part of the Article traces the development of workplace privacy as a fundamental right and explains how it is that European workers enjoy

---

Fine Line Dividing the Prudently Managed Enterprise from the Modern Sweatshop, 41 DEPAUL L. REV. 739, 808 (1992) (quotation omitted).

12. The term 'electronic sweatshop,' in reference to the impact of computers, was first conceptualized by Barbara Garson. *See* BARBARA GARSON, THE ELECTRONIC SWEATSHOP (1988) (describing the ways that computers infringe upon privacy). *See also* Laurie Thomas Lee, *Watch Your E-mail! Employee E-mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop,"* 28 J. MARSHALL L. REV. 139, 139 (1994) (noting that e-mail is the "fastest growing form of electronic communication in the workplace").

13. Matthew W. Finkin, *Menschenbild: The Conception of the Employee as a Person in Western Law*, 23 COMP. LAB. L. & POL'Y L. J. 577, 577 (2002).

14. *See* Lawrence E. Rothstein, *Privacy or Dignity? Electronic Monitoring in the Workplace*, 19 N.Y.L. SCH. J. & INT'L & COMP. L. 379, 379 (2000) ("The growth of electronic surveillance in the workplace has been phenomenal and has created a global problem.").

greater privacy in the workplace. The countries of the European Union (E.U.) have adopted what in effect is a human rights model that arms employees with countervailing privacy rights to challenge abusive employer surveillance practices.[15] The result is that the U.S. and Europe have diametrically opposed approaches to workplace privacy.

Next, we examine two parallel bodies in Europe that formulate policy relevant to privacy and other human rights: the Council of Europe and the European Union. These transnational institutions have played a major role in shaping the "human rights" approach adopted for European electronic monitoring. To illustrate the divergent approaches, the American law of electronic monitoring is compared to developments in France, a civil law jurisdiction, and the United Kingdom, which adheres to the common law tradition. In these and other countries of the European community, there is a concerted attempt to balance the employers' need to monitor with workers' fundamental rights of privacy. Part III proposes that Congress enact an Electronic Monitoring Act to give all U.S. workers written and electronic notice prior to employer monitoring of electronic communications. The proposed act would provide for consequential damages and punitive damages, as well as attorney's fees, if employers were to engage in clandestine monitoring.

The Electronic Monitoring Act would punish and deter companies that abuse the privilege of electronic monitoring of employee communications and computer usage in the workplace. By adopting this reform, companies would have, in effect, a safe harbor in cross-border communications with their European trading partners. This proposed limited legal reform is only the first step in preventing U.S. companies from devolving into electronic sweatshops. Gone should be the days when American workers have no privacy in their e-mails and Internet usage.

II. WORKPLACE PRIVACY IN THE U.S. ELECTRONIC WORKPLACE: THE PROPERTY-BASED APPROACH

> Americans reflexively dismiss Europe as a clapped-out old continent—a wonderful place to visit but hardly the anvil of the future. Europeans, equally reflexively, dismiss America as the embodiment of all the evils of modernity—a testosterone-driven adolescent bereft of history and tradition.[16]

---

15. Gail Lasprogata et al., *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. 4 at ¶ *8 (2004).

16. *Old America v New Europe*, ECONOMIST, Feb. 22, 2003, at 32.

The United States and Europe have clashing concepts of privacy in the protection of personal information.[17] In general, Europe has a basic set of legal protections not found in the United States. The first section of Part I illustrates this great divide through the help of a hypothetical about PhDog.com, a multinational company with operations in the United States and Europe, as a pedagogical device for comparing and contrasting the U.S. property-rights regime with the Europeans' human rights approach to electronic surveillance. The property-rights approach holds that since "employers own the work tools, they can initiate surveillance at will."[18] The twin rationales underlying the property-rights approach are:

"[1] Employees have no reasonable expectation of privacy when using company e-mail/Internet facilities.

[2] The employer's ownership of these work tools entitle her to monitor their use in any way she deems fit."[19]

The first section explains the justifiable reasons employers have for monitoring the e-mail or Internet usage of their workers. The next sections of Part I trace the constitutional, common law, and statutory legal frameworks governing U.S. workplace monitoring of electronic communications.

A. The PhDog.com Hypothetical for Transnational Electronic Surveillance

You are a recent graduate from Big Eastern Law School and have been hired as an associate in a Boston law firm known for its expertise in advising multinational corporations. Your law firm received a call from the corporate counsel of PhDog.com (PhDog), a multinational software sales and services company located at 120 Tremont Street in downtown Boston. Your law firm has been asked to advise PhDog on a number of employment issues regarding the company's monitoring of electronic mail and Internet usage in the U.S. and at its overseas subsidiaries in Nice, France.

A senior partner in your firm has also asked you to research and prepare a memorandum regarding the legal issues arising out of PhDog's electronic surveillance of its employees in the United States and at its

17. Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 718 (2001).

18. Karen Eltis, *The Emerging American 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).

19. *Id.*

French subsidiary. PhDog's business plan is to introduce a revolutionary new business method throughout Europe that will allow seamless cross-border transfers of software and other intangibles. The information-based company has invested much of its financial and human capital into its innovative business plan. PhDog's Chief Executive Officer, on the advice of counsel, requires all of its employees to sign a nondisclosure and confidentiality agreement acknowledging the confidential nature of the business plan.

PhDog is concerned that its employees may be committing torts and crimes while surfing and chatting online when they are supposed to be working.[20] The company has the foremost concern that its employees use information technology to transfer business plans, product designs, and other intangible assets.[21] To protect its business plan, proprietary information and other trade secrets, PhDog has surreptitiously installed an e-mail spy software product called "On the Sly," which tracks all of the e-mail and Internet activities of its employees. On the Sly monitors all outgoing and incoming e-mail, as well as the employees' general Internet use. The clandestine software is configured to detect all transmissions in multiple languages, including French and English. PhDog's corporate counsel is concerned about a case that he read in which the Supreme Court of France decided that employers did not have the right to read their employees' e-mails or capture other electronic records.[22]

An audit of the first six months of online surveillance at PhDog has yet to unearth evidence that company employees are misappropriating trade secrets or other intangible assets. On the Sly's audit tracking program reveals that one of the company's senior managers visited the website of a popular erectile dysfunction drug and another investigated options for assisted living. Another disconcerting audit trail revealed that a trusted systems analyst was unveiled as an occasional user of pornography, according to the keystroke tracking function.[23] Another PhDog employee was furtively using his business computer to enroll and pay for his membership in a new age religion. A different employee was using the office computer to participate in a web blog critical of a new age religion.[24]

---

20. *See* Jay P. Kesan, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 290 (2002) ("It's estimated that 'cyberslacking' is responsible for up to a 40% loss in employee productivity and can waste up to 60% of a company's bandwidth!") (quotation omitted).

21. IDG.net, *Employers Fear Litigation Over E-mail* (Sept. 26, 2001), *at* http://www.nua.ie/surveys/?f=VS&art_ id=905357234&rel=true.

22. Nikon France v. Onos, Cass. Soc. Arret No. 41-6410/2/01 (France 2001).

23. *See* Susan E. Gindin, *Guide to E-Mail and the Internet in the Workplace*, BNA Corporate Practice Series, at 1 (1999) (noting that the surfing of online pornography is a common abuse in the workplace).

24. Company employees may create potential lawsuits by sending e-mails denigrating

Still other PhDog employees were found to have visited WebMd.com and downloaded information on maladies such as depression, diabetes, and hypertension. PhDog's CEO was enraged when he learned that employees were discussing a long term relationship he had with his secretary. On the Sly's tracking software documented that many PhDog employees extensively play online videogames and download movies and music during work hours.

PhDog's corporate counsel is concerned that a former employee of its Nice branch has been mass e-mailing the company's current French employees. The e-mails charge the company with violating French labor laws. PhDog's computer experts have been unable to block these uninvited e-mails because the former employee adroitly circumvents firewalls as well as blocking software. The ex-employee has been participating with a group of current employees in making disparaging remarks about PhDog's business practices on the union's website.

Further, it appears that a number of other PhDog employees are routinely surfing pornographic sites and circulating links to sexually explicit websites around the office. PhDog's Chief Executive Officer is considering terminating twenty employees for misusing the company's Internet and e-mail systems. These employees are based both in Nice, France and Boston, Massachusetts. You have been appointed as corporate counsel for PhDog and have been asked about PhDog's rights, remedies and potential liability regarding intrusive e-mail or Internet monitoring.

The development of new information technologies has given PhDog enhanced access to information, but it also creates the likelihood of widespread misuse of the Internet in the workplace. The downside is that a company like PhDog can lose its business plans, trade secrets, and other proprietary information at a click of the mouse. PhDog's corporate counsel approved the installation of On the Sly and takes the position that the company owns the computers and pays for the Internet connections. Since PhDog's employees have no property rights in the computers or their contents, they have no reasonable expectation of privacy.[25]

---

or even advocating religious ideologies. *See, e.g.*, Curtis v. DiMaio, No. 99-7468, 2000 U.S. App. LEXIS 902, at *2 (2d Cir. Jan. 25, 2000) (affirming lower court's dismissal of hostile workplace claim based primarily upon co-employees sending ethnically charged e-mails). In *Sattar v. Motorola, Inc.*, 138 F.3d 1164 (7th Cir. 1998), a company was sued when a supervisor sent a co-employee hundreds of thousands of e-mails warning him of the consequences of turning his back on the Islamic religion. Even though the company prevailed in the *Sattar* case, the litigation was high-priced and time-consuming.

25. *See, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (finding that there is no reasonable expectation of privacy in e-mail communications); McLaren v. Microsoft, No. 05-97-00824-CV, 1999 Tex. App. LEXIS 4103, at *12 (Tex. App. 1999) (holding that employees had no expectation of privacy in e-mail).

B. The Justification for E-Mail & Internet Usage Monitoring

The PhDog.com hypothetical illustrates the critical importance of privacy issues in the electronic workplace.[26] Part I of this Article will cover the U.S. constitutional, common law, and statutory provisions that our young associate will need to consider. Our new law associate will need to familiarize herself with the legitimate reasons why companies like PhDog.com need to keep an eye on their employees' e-mail and Internet usage. Despite the multiplicity of reasons for monitoring employee e-mail and Internet usage, the unifying theme is that electronic surveillance is necessary to reduce the risk of vicarious corporate liabilities for companies like PhDog.com.[27] This section addresses the legal troubles a company like PhDog.com will have if its employees abuse e-mail and Internet usage as described in the hypothetical.

PhDog.com's officers must be alert to the fact that their employees' e-mail messages tend to be more informal than formal business letters. In contrast to a formal business letter, e-mail tends to be more incendiary and can expose the company to potential liability. Another risk with e-mail is that it can be forwarded easily throughout and beyond the company with the click of the mouse. Monitoring e-mail or Internet usage is justified, because the mishandling of these technologies is not a phantom risk. Since the invention of the Internet, there have been a large number of lawsuits against employees for the abuse of e-mail or the Internet, as this section demonstrates.

Companies posit many reasons for electronic surveillance, including: [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.[28]

---

26. *See generally* Lee, *supra* note 12, at 139 ("Employee privacy is considered to be the most significant workplace issue facing companies today.").

27. *See generally* Erin M. Davis, Comment, *The Doctrine of Respondeat Superior: An Application to Employers' Liability for the Computer or Internet Crimes Committed by Their Employees*, 12 ALB. L.J. SCI. & TECH. 683 (2002) (explaining the liabilities employers face as a result of their employees' unmonitored use of the Internet).

28. Lasprogata et al., *supra* note 15, at ¶ *3; *see also* Govan & Mac, *supra* note 3, at

There is also a significant issue regarding what steps the company should take to limit the use of computers for personal use. Here, PhDog's corporate counsel is concerned with productivity issues as opposed to legal liabilities. A study of Internet usage in the workplace found that "[a]mong the top-ten-most-visited sites by workers during work hours in January 2000 were the eBay auction site (157 minutes); the Datek (120 minutes); the Charles Schwab (86 minutes), E-trade (66 minutes) and Fidelity Investments (63 minutes) investment sites; and the personal interest sites RootsWeb (61 minutes) and MyFamily.com (58 minutes)."[29]

Employees can also use e-mail to solicit and harass co-workers or transmit confidential business plans to competitors. Rogue employees can place PhDog at risk for liability for creating a hostile work environment. However, as PhDog licenses software and renders services, its chief reasons for monitoring its workers are to protect its intellectual property assets and to avoid infringing the intellectual property rights of others.

1. Reducing Hostile Workplace Claims

PhDog.com may become ensnared in expensive and prolonged litigation because of the documented problem of its employees surfing pornographic sites and sending links to sexual explicit websites to co-workers. A growing number of U.S. companies monitor e-mail and Internet communications to reduce exposure for the online torts of their employees. Employer-provided computer systems may result in "claims of discrimination or sexual harassment arising from . . . employees' sexual, racial, or otherwise threatening or harassing e-mails or Internet graphics or messages, as well as for defamation, copyright infringement, fraud or other claims related to employee misconduct."[30]

E-mail jokes, ribald screensavers, or the downloading of pornography may also expose an employer to sexual harassment lawsuits. Sexually charged e-mails were the basis of a harassment claim against the *Chicago Sun-Times* newspaper.[31] The smoking gun in the *Chicago Sun-Times* case was an incendiary e-mail from a supervisor that stated: "I know I'm getting to be a pain [in] the butt with these ride offers. And I apologize. But I can't help myself."[32] In another case, an employee's sexual

252 (citing a study which found that twenty-two percent of employers monitored their employees' electronic communications and activity).

29. Goven & Mac, *supra* note 3, at 252.

30. Mark E. Schreiber, *Employer E-Mail and Internet Risks, Policy Guidelines and Investigations*, 85 MASS. L. REV. 74, 74 (2000).

31. Greenslade v. Chicago Sun-Times, Inc., 112 F.3d 853, 868–69 (7th Cir. 1997) (affirming dismissal of employee's Title VII claim alleging sexual harassment via e-mail).

32. *Id.* at 864 (alteration in original).

harassment claim was based in part on an e-mail message from a co-employee asking the plaintiff whether she wanted to enjoy a "horizontal good time" together.[33]

2. Preventing the Loss of Intellectual Property Rights

PhDog's crown jewels are its intangible intellectual property rights, such as new product designs, software codes, and business customer lists. While the On the Sly audit has uncovered no direct evidence of theft of intellectual property by employees, audit trails will document any future unauthorized transfers. Apart from harassment claims, the greatest hazard is the possibility that employees or former employees will use company computers to divulge trade secrets. A spiteful ex-employee may have not surrendered passwords or other authentication devices, giving him the power to make files and records disappear with the push of a button.[34] E-mail gives computer users the means to transmit data files, pictures, and even videos instantaneously. These illicit transfers can jeopardize the trademarks, patents, copyrights and trade secrets critical to executing PhDog.com's business plan.

A company that does not monitor its trade secrets may lose its most valuable assets. Once revealed, proprietary information loses its status as a trade secret, which is defined as any information "including a formula, pattern, compilation, program, device, method, technique, or process" that has independent economic value.[35] Electronic surveillance is a reasonable means to maintain the secrecy of PhDog's intangible assets.

PhDog.com is not only concerned with the loss of its own intellectual property, but seeks to avoid liability to others. A substantial risk is that the company will be subject to unfavorable publicity, if not legal liability, from its employees' downloading of unauthorized copies of copyrighted software, music or entertainment on office computers. Peer-to-peer file sharing programs allow Internet users to connect directly to one another's computers and exchange files indiscriminately, violating copyright and trademark rights. This type of file exchange was the subject of the famous Napster litigation.[36]

File-swapping software is heedless to PhDog.com's firewalls and allows employees to swap copyrighted software, images, and video on the

33. Knox v. Indiana, 93 F.3d 1327, 1330 (7th Cir. 1996).

34. *See, e.g.*, United States v. Martin, 228 F.3d 1 (1st Cir. 2000) (affirming criminal conviction of employee who conspired via e-mail to steal trade secrets from a veterinary laboratory); James Garrity and Eoghan Casey, *Internet Misuse in the Workplace: A Lawyer's Primer*, 72 FLA. B. J. 22 (Nov. 1998).

35. UNIF. TRADE SECRETS ACT § 1(4) (2004).

36. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

company's network with impunity. It is unclear whether the company would be exposed to contributory copyright liability, but the publicity of such a lawsuit would likely be negative and the expenses of litigation very great.

In addition, PhDog.com may be liable for corporate espionage if there is proof that an employee accessed a competitor's computer system without authorization. PhDog.com will not normally be liable for its employees' knowing release of a virus computer code. PhDog is not likely to be vicariously liable for its employees' cybercrimes absent facts proving that high-level officials ratified or acquiesced in illegal computer surveillance of competitors. The next section examines PhDog's possible exposure to employee lawsuits based upon constitutional, statutory and common law theories.

C. *Constitutional Protection against Workplace Monitoring*

1. Federal Constitutional Developments

The framers of the U.S. Constitution could not have anticipated the degree to which new technologies could erode the privacy of all Americans. F. Scott Fitzgerald's metaphor of Dr. Eckleberg's omniscient gaze symbolizes how far-reaching technologies strip workers of their privacy through new tools and technologies.[37] The U.S. Constitution did not explicitly address privacy as a fundamental right, nor did the Founding Fathers focus on the private sphere.[38] However, the Supreme Court has recognized a right of privacy in the decision to have and to rear a child.[39] In general, the Constitution recognizes privacy as a penumbral theory.[40] The right of privacy has not yet evolved to protect employees' electronic communications. As Erwin Chemerinsky notes:

> Most Americans would be surprised to learn that there is no right to privacy granted in the United States Constitution. The Fourth Amendment protects privacy in limiting police searches and

37. FITZGERALD, *supra* note 7.

38. *See* MADELEINE SCHACHTER, INFORMATIONAL AND DECISIONAL PRIVACY 8 (2003) ("Constitutional privacy law has evolved largely from textual and inferential construction of the Bill of Rights; in particular, the First, Fourth, Fifth, and Ninth Amendments, as well as the Fourteenth Amendment.").

39. The Court has ruled that there is a right of privacy that encompasses the right of a woman to terminate a pregnancy. Roe v. Wade, 410 U.S. 113 (1973). Similarly, the government does not have the discretion to supplant parental rights to make decisions concerning a child's education. Runyon v. McCrary, 427 U.S. 160 (1976).

40. *See* SCHACHTER, *supra* note 38, at 79 (quoting the penumbral theory of Justice William O. Douglas in *Griswold v. Connecticut*, 381 U.S. 479 (1965)).

> arrests, but privacy in terms of autonomy and the right to be let alone by the government is not mentioned in the text of the Constitution.[41]

To put it bluntly, PhDog's employees have no constitutional protections against PhDog's electronic surveillance because of the doctrine of state action.[42] Constitutional protection does not extend to PhDog's employees because they are in the private workplace. In the United States, private employees have no constitutional right to privacy in the workplace because they cannot satisfy the state action requirement.[43]

The seamy side of electronic surveillance is that it infringes upon the fundamental right of employees.[44] An empirical study demonstrates that workers who were electronically monitored manifested higher rates of depression, anxiety, and fatigue than others in the same business that were not monitored.[45] This research confirms that the very system that is supposed to protect the employer to ensure efficiency can actually

---

41. Erwin Chemerinsky, *Privacy and the Alaska Constitution: Failing to Fulfill the Promise*, 20 ALASKA L. REV. 29, 29 (2003) (citations omitted).

42. In e-mail monitoring the plaintiff has the burden of proving that the state directed or controlled electronic surveillance in order for constitutional rights to be triggered:

> Central to the understanding of privacy rights in the American workplace is the public/private distinction. Simply put, the extent of employees' privacy rights in the workplace depends on whether they work in the public sector or private sector. Because constitutional rights operate primarily to protect citizens from the government, "state action" is required before a citizen can invoke a constitutional right. The manner in which a government employer treats its employees is by definition state action. Because of this dichotomy, public-sector employees enjoy far greater privacy rights than do private-sector employees. For example, the Fourth Amendment protects all government workers from unreasonable searches and seizures by the government.

S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace*, 32 GA. L. REV. 825, 828 (1998) (citations omitted). *See also* Kevin J. Conlon, *Privacy in the Workplace*, 72 CHI.-KENT L. REV. 285, 286 (1996) ("The Court has been reluctant to find state action in the private sector . . . ."); MacDonald v. Eastern Wyoming Mental Health Center, 941 F.2d 1115, 1118 (10th Cir. 1991) (holding that "[a]bsent any showing that the state directed, controlled, or influenced this particular personnel decision," proof that the private agency was subject to pervasive state regulation and monitoring of its personnel standards and received substantial state funds was not sufficient to show state action).

43. *See generally* John Araneo, Note, *Pandora's (E-Mail) Box: E-Mail Monitoring in the Workplace*, 14 HOFSTRA LAB. L. J. 339 (1996) (discussing the lack of federal constitutional protection for individual privacy).

44. *See generally* Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 958 (1989) (arguing that privacy is a domain value in response to an increasingly intrusive society).

45. Peter Blackman & Barbara Franklin, *Blocking Big Brother: Proposed Law Limits Employer's Right to Snoop*, N.Y.L.J., Aug. 19, 1993, at 5.

demoralize the electronic workplace.

U.S. employees have no constitutional remedy against private employer monitoring, even if it is implemented in a discriminatory fashion without notice. In contrast, employees in the public sector have some constitutional protection against abusive monitoring because public employers are subject to constitutional constraints, such as the right to reasonable searches and seizures.[46] Under specific factual settings, courts have ruled that a public sector employee has an expectation of privacy in sent or received e-mail or Internet communications.

The Fourth Amendment protects a person in the governmental workplace only if he has proved a subjective as well as an objective expectation of privacy in the place searched.[47] In *Leventhal v. Knapek*,[48] a Department of Transportation investigation uncovered evidence of an employee's misuse of a computer. The Second Circuit recognized that the employee had a reasonable expectation of privacy, but concluded that the investigatory search did not violate his Fourth Amendment rights because the employer's privacy interest was outweighed by the government's legitimate purpose in conducting the search.[49] The Fourth Amendment does not apply to a search unless the governmental intrusion infringes on the plaintiff's reasonable expectation of privacy, which is the legally protectible interest.

The *Knapek* court validated the investigatory search because it was reasonable in scope and advanced the employer's legitimate objective of searching for evidence of employee misfeasance.[50] In the United States, courts balance privacy concerns against the employer's interest in the public sector, but they do not apply this balancing test to the private sector workplace. The European approach, like the U.S. public sector due process framework, offers procedural protections against the employer's workplace surveillance of e-mail and Internet activities, but with the difference that Europe has procedural protections for both public and private employees.

---

46. *See* O'Connor v. Ortega, 480 U.S. 709 (1987) (finding that the strictures of the Fourth Amendment apply to government employers).

47. The Fourth Amendment provides "[t]he right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. CONST. amend. IV; *see* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (explaining that the Fourth Amendment applies to protect privacy where there is, both subjectively and objectively, a reasonable expectation of privacy); *O'Connor*, 480 U.S. at 716 (1987) (applying the Fourth Amendment to searches in public sector workplaces).

48. 266 F.3d 64 (2d Cir. 2001).

49. *Id.* at 75.

50. *Id.*

2. State Constitutional & Statutory Developments

In the United States, the right of privacy was not enumerated in the Constitution and did not evolve until the twentieth century. States vary significantly in the degree of constitutional protection given to privacy-based interests. Article I, section 22 of Alaska's constitution states that "[t]he right of the people to privacy is recognized and shall not be infringed."[51] Montana's constitution also recognizes a right to privacy that potentially applies to e-mail monitoring.[52] However, to date, no court has extended state constitutional rights of privacy to e-mail monitoring or electronic surveillance.[53]

Delaware enacted a statute that requires employers to give their employees notice before monitoring their e-mail or Internet usage.[54] Employers can comply with the Delaware statute by providing employees with "an electronic notice of monitoring policies or activities" each time they access their business computers.[55] The employer can also comply with the statute by giving a "1-time notice" to the employee in writing or in electronic form that must be acknowledged by the employee.[56] Connecticut requires employers to give employees notice prior to e-mail or Internet monitoring.[57] New York recognizes the right of publicity, but not the other privacy-based torts such as intrusions upon seclusion.[58] New York's statute would extend to workers whose right of publicity was infringed upon by electronic monitoring.

In 2000, the California Senate passed the legislation that would have required all employees to receive electronic as well as hard copies of all employers' electronic monitoring policies.[59] In addition, employees would either sign or manifest assent electronically that they had "read, understood and received the employer's monitoring policies and practices."[60] While the proposed statute would permit employers to access personally identifiable information of employees, an employer's "violations of the

51. ALASKA CONST. art. 1, §22.

52. Mark S. Kende, *The Issues of E-Mail Privacy and Cyberspace Personal Jurisdiction*, 63 MONT. L. REV. 301 (2002).

53. Corey A. Ciocchetti, *Monitoring Employee E-Mail: Efficient Workplaces vs. Employee Privacy*, 2001 DUKE L. & TECH. REV. 26 at ¶10.

54. DEL. CODE ANN. tit. 19, § 705 (2005).

55. DEL. CODE ANN. tit. 19, § 705(b)(1).

56. DEL. CODE ANN. tit. 19, § 705(b)(2).

57. DAVID W. QUINTO, THE LAW OF INTERNET DISPUTES § 11.03[A] at 11-59 (2002).

58. N.Y. CIV. RIGHTS § 50 (2005) ("A person, firm or corporation that uses for advertising purposes, or for the purposes of trade, the name, portrait or picture of any living person without having first obtained the written consent of such person, or if a minor of his or her parent or guardian, is guilty of a misdemeanor.").

59. QUINTO, *supra* note 57, at 11-59.

60. *Id.* at 11-60.

prohibition on secret monitoring would have been treated as a misdemeanor."[61] The California statute was vetoed by then-Governor Gray Davis on the grounds that employees already understood that they could be monitored while using business computers.[62] The vast majority of states have no statutes or case law requiring employers to give employees notice or any other procedural right prior to instituting electronic surveillance.

D. Tort Law Remedies for E-Spying

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. First, we will describe the evolution of privacy law and how to classify e-mails under those laws. Second, we will examine the relevant federal statutes and case law. The cases will be divided into those where the company has an e-mail and Internet usage policy and those where it does not. This distinction will have a major impact on our comparison with Europe, as we will show in Part II.

1. The Origin of Privacy as a Tort

Louis Brandeis and his law partner, Samuel Warren, first proposed a new tort action for the invasion of privacy in a Harvard Law Review article in 1890.[63] The principal reason that Warren and Brandeis wrote their article was to propose new remedies for abuses by the print media. Their article was influential in convincing the states to recognize privacy-based torts.[64] "It has been said that a 'right of privacy' has been recognized at common law in 30 States plus the District of Columbia and by statute in

61. *Id.*

62. *Id.*

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

64. The U.S. Supreme Court, in *Time, Inc. v. Hill*, 385 U.S. 374 (1967), noted how New York's privacy statute was enacted a year after *Roberson v. Rochester Folding Box Co.*, 171 N.Y. 538, 64 N.E. 442 (1902).

> The New York Court of Appeals traced the theory [of the right to privacy] to the "celebrated article of Warren and Brandeis, entitled The Right to Privacy . . . The Court of Appeals, however, denied the existence of such a right at common law but observed that "[t]he legislative body could very well interfere and arbitrarily provide that no one should be permitted for his own selfish purpose to use the picture or the name of another for advertising purposes without his consent."

Time, Inc., 385 U.S. at 380–81 (quoting *Roberson*, 171 N.Y. at 545).

four States."[65] The U.S. Supreme Court drew upon Warren and Brandeis in articulating the right to privacy as "[the] right to be let alone."[66] This newly-minted "right to be left alone" was an extension of the right to life, or rather the right to enjoy life without the interference of outside intervention. However, it was not until 1960 that William Prosser formulated four different theories to support a claim for invasion of privacy: (1) intrusion upon seclusion; (2) appropriation of another's name or likeness; (3) false light; and (4) publication of private facts.[67] Intrusion upon seclusion is the most relevant of the privacy-based torts to the electronic workplace.[68] In the past forty-five years, the majority of jurisdictions have recognized these four privacy-based torts through either statute or case law.[69] However, these privacy-based torts have yet to be extended to punish and deter the unreasonable surveillance of employees in the private workplace.

2. Extending Privacy-Torts to E-Mail Surveillance

In the early years of the Internet, it was unclear how e-mail should be classified because it was a hybrid medium with attributes of several different means of communication. The issue was whether e-mails were functionally equivalent to the telegraph, letters, postcards, phone calls, or radio communications. Courts have long recognized that employees have an expectation of privacy in ordinary mail. In the 1878 case of *Ex Parte Jackson*, the *habeas corpus* petitioner was indicted for violating the U.S. Revenue Code after postal agents seized circulars for a lottery he sent through the mail.[70] The *Jackson* Court distinguished regular mail intended to be kept free from inspection, such as letters and sealed packages, from newspapers, pamphlets and postcards, which could be inspected or even read by postal inspectors without being opened.[71] The court noted that if

65. *Time, Inc.*, 385 U.S. at 383 (citing WILLIAM L. PROSSER, LAW OF TORTS 831–32 (3d ed. 1964)).

66. Katz v. United States, 389 U.S. 347, 350 & n.6 (1967).

67. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960); W. PAGE KEETON ET AL., PROSSER AND KEETON ON TORTS § 117 (5th ed. 1984).

68. *See* Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996) (holding that even if the employee had a reasonable expectation of privacy, a reasonable person would not find the interception of such communications to be intrusive).

69. RESTATEMENT (SECOND) OF TORTS § 652A (1977).

70. 96 U.S. 727 (1877).

71. In their enforcement, a distinction is to be made between different kinds of mail matter,—between what is intended to be kept free from inspection, such as letters, and sealed packages subject to letter postage; and what is open to inspection, such as newspapers, magazines, pamphlets, and other printed matter, purposely left in a condition to be examined. Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as

the inspector opened a closed letter, the sender's expectation of privacy would be violated, but there was no violation in reading mail open to view.[72]

One commentator contends, "Opening an employee's mail clearly marked 'personal' invades privacy; opening mail only to ascertain if it concerns the business would not."[73] In *Vernars v. Young*, [74] a corporate officer opened mail that was marked "personal" and addressed to an employee. The defendant read the personal communication and then promptly terminated the plaintiff. The plaintiff claimed that the defendant "fraudulently misappropriated corporate funds for his personal benefit."[75] The plaintiff was not only an officer, but a shareholder of the corporation. The defendant owned 50% of the stock and was a principal officer of the corporation.[76] The *Vernars* court reasoned that private individuals had a reasonable expectation that their personal mail, addressed to them and marked personal, would not be opened and read by unauthorized persons, even if the mail was delivered to the corporation's office.[77] To date, no court has extended this same logic to distinguish between personal and business e-mail communications.

> to their outward form and weight, as if they were retained by the parties forwarding. . . . The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household.

Id. at 732–33.

> 72. No law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail; and all regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the fourth amendment of the Constitution.

Id. at 733.

73. Matthew W. Finkin, *Employee Privacy, American Values and the Law*, 72 CHI.-KENT. L. REV. 221, 225 (1996).

74. 539 F.2d 966 (3d Cir. 1976).

75. *Id.* at 967.

76. *Id.*

77. The court found that the plaintiff had met her burden of showing evidentiary support for the tort of intrusion upon seclusion: "[o]ne 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 man." *Id.* at 969 n.1 (quoting RESTATEMENT (SECOND) OF TORTS § 652B) (1977).

E. Stretching the ECPA to E-Mail Surveillance

In American culture, the greatest concern about invasion of privacy has come from surveillance by the federal government rather than monitoring in private sector workplaces where the Constitution does not apply. In public sector employment cases, the Fourth Amendment may apply in certain circumstances. After a controversial early ruling on wiretapping,[78] Congress enacted the Federal Communication Act of 1934 (FCA). Section 605 of the FCA prohibited unauthorized interception of any communication and unveiling or publication of the existence, content, substance, purpose, effect or meaning of such intercepted communication, unless the sender had consented.[79]

Congress developed specific guidelines governing interceptions by law enforcement officers in Title III of the Omnibus Crime Control and Safe Streets Act of 1968, also know as the Federal Wiretap Act.[80] The Federal Wiretap Act applied to both federal and state officials.[81] In 1986 Congress modernized the Federal Wiretap Act and enacted the Electronic Communications Privacy Act of 1986 (ECPA) to extend privacy protection to "wire" and "oral" communications.[82] However, Congress amended the Federal Wiretap Act when it enacted the USA Patriot Act.[83] The USA Patriot Act permits federal government agents to intercept e-mail and monitor other Internet activities.[84] E-mail falls within the scope of the ECPA so long as the information technology has a substantial nexus to

78. Olmstead v. United States, 277 U.S. 438 (1928) (holding that there is no Fourth Amendment protection since the interception involved no physical intrusion on plaintiff's property).

79. This section applied to wire communications and wiretapping, but not to bugging or eavesdropping.

80. The Omnibus Crime Control and Safe Streets Act (The Federal Wiretap Act or Title III), Pub. L. No. 90-351, (codified at 18 U.S.C. §§ 2510–2520 (1968)).

81. 18 U.S.C. § 2510(7).

82. 18 U.S.C. § 2510.

83. A "wire communication" under the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510, was "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception" and includes any electronic storage of such communication. 18 U.S.C. § 2510(1). However, this provision has been superseded by the USA Patriot Act. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act, Pub. L. No. 107-56, § 209, 115 Stat. 272, 283 (Oct. 26, 2001) (striking electronic storage of communications from the definition).

84. *See* USA Patriot Act § 202 (amending 18 U.S.C. § 2516(1) to list crimes for which investigators may obtain a wiretap order for wire communications). The USA Patriot Act also amended the felony violations of 18 U.S.C. § 1030 to the list of predicate offenses to warrant wiretapping. *See* 18 U.S.C. § 2516(1) (explaining procedures for government interception of electronic communications to combat terrorism).

interstate commerce. Title I of the ECPA prohibits "interception" of electronic communications such as telephone calls and e-mail.[85] Title II provides guidance on what constitutes unlawful access and disclosure of communications in electronic storage, e.g., messages left on voice machines.[86] One court observed that "the intersection of these two statutes is a complex, often convoluted, area of the law."[87] ECPA's legislative history does support the argument that e-mail, as a form of electronic communication, is to be given privacy protection.[88] The next part of this section will examine how courts have construed the ECPA in the employment context.

1. Federal Statutory Protection under the ECPA

a. Title I of ECPA – Federal Wiretap Statute[89]

The ECPA prohibits only "interceptions" of electronic communications.[90] "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[91] The ECPA makes it a crime to intercept a wire, oral, or electronic communication.[92] Under Title I of the Wiretap Act there are three types of activities that are prohibited: (i) intercepting or endeavoring to intercept electronic communications, (ii) disclosing or endeavoring to disclose intercepted information, and (iii) using the content of intercepted information.[93] Therefore, an employer who monitors e-mail or intercepts Internet communications has intercepted electronic communications within the meaning of the ECPA.[94]

---

85. 18 U.S.C. § 2510(4). The Federal Wiretap Act defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature [with limited exceptions]. . . ." 18 U.S.C. § 2510(12). In the Act, Congress made no mention of electronic storage of electronic communications. *See also* U.S. v. Councilman, 373 F.3d 197, 209 (1st Cir. 2004) (reasoning that Congress intended to exclude stored communications from the scope of the Federal Wiretap Act).

86. Electronic storage includes a vast range of possible situations including any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof. *See* United States v. Councilman, 373 F.3d 197, 201 (1st Cir. 2004) (citing 18 U.S.C. § 2510(17)(A)).

87. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. filed Aug. 23, 2002) (quotation omitted).

88. *See* S. Rep. No. 99-541, at 14 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568 (stating that the term "electronic communications" also includes e-mail).

89. Codified at 18 U.S.C. §§ 2510–2511 (2000).

90. 18 U.S.C. § 2511.

91. 18 U.S.C. § 2510(4).

92. 18 U.S.C. § 2511(1)(a).

93. 18 U.S.C. § 2511.

94. 18 U.S.C. § 2511.

The interception has to be intentional, which means that the person committing the interception has to know or have reason to know that the information has been illegally intercepted.[95] Electronic communications, including e-mails, are all communications that do not constitute wire or oral communications.[96] Third parties are allowed to monitor the transactional information of the e-mail such as who the sender and recipient are, the date and time, and the length and subject heading of the message.[97] Title I only protects the content of the messages when they are under transmission.[98] This means that Title I is inapplicable to an employer's search of an employee's stored e-mail messages.[99]

There are two statutory exceptions under Title I that apply to electronic communications in the employment context. First, the ECPA permits service providers or anyone else to intercept and disclose an electronic communication where either the sender or recipient of the message has effectively consented to disclosure, either explicitly or implicitly.[100] Consent, as defined by the ECPA, also encompasses implied consent, "which, in the case of monitoring of employees, may be achieved when an employer gives prior notice to its employees that it will monitor e-mail communications."[101] Second, there is an "ordinary course of business" exception, which may in certain circumstances allow employers to monitor their employees' e-mail.[102]

To meet the ordinary course of business exception, the employer has to demonstrate that: (i) the device used to intercept the electronic communication is "a telephone or telegraphic instrument, equipment or facility, or any component thereof," either provided or installed by the employer, and (ii) that the device is used by the employer within the ordinary course of the business.[103] However, the employer is only allowed to intercept long enough to determine the nature of the communication. If

95. 18 U.S.C. § 2511(1).

96. DAVID SOLOVE & MARK ROTENBERG, INFORMATION PRIVACY LAW 330 (2003).

97. 18 U.S.C. § 2511.

98. 18 U.S.C. § 2510(1).

99. *See* Thomas R. Greenberg, Comment, *E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 AM. U. L. REV. 219, 248 (1994) ("The distinction between the terms 'intercept' and 'access'. . . is critical when a transmitted communication is later electronically stored . . . . This is the case with both E-mail and voice mail messages, both of which have a transmission phase and a storage phase. During the transmission phase, any protection against unlawful interception . . . is governed by § 2511. On arrival in storage, the same messages are subject to § 2701.").

100. 18 U.S.C. § 2511(2)(d).

101. Frank C. Morris, Jr. & Jennifer S. Recine, *The Electronic Platform: The Implications of Technology in the Workplace*, SKO13 ALI/ABA 1153, 1159 (July 29, 2004).

102. 18 U.S.C. § 2510(5)(a)(i).

103. 18 U.S.C. § 2510(5)(a).

the communication is personal, the employer must cease and desist from intercepting the communications further.[104]

The Sixth Circuit refused to apply the "ordinary course" exception of the ECPA in *Adams v. City of Battle Creek*.[105] In *Adams*, a city police department secretly monitored and tapped a department-supplied pager of one of its officers. In that case, the police department had the erroneous belief that its officer was assisting drug dealers. The court held that the Department did not qualify for the "ordinary course of business" exception given that the officer had no notice of the monitoring.[106] The court reasoned that the ordinary course exception required that the use be (1) for a legitimate business purpose, (2) routine, and (3) with notice.[107] The court rejected the department's argument that it had a reason to monitor the pager because of the department's general prohibition against the personal use of these devices. The court reasoned that this was an after-the-fact justification for intercepting the plaintiff's pager, especially where the policy had not been enforced and the department was aware that many officers had used pagers for personal use. The court reasoned that "[w]hat is ordinary is apt to be known; it imports implicit notice."[108] The court found that the department did not fall under any one of the statutory exclusions provided by the federal wiretapping laws.[109]

In *Arias v. Mutual Central Alarm Services, Inc.*,[110] former employees of an alarm services firm sought monetary damages against their employer for intercepting telephone conversations under the federal wiretap statute.[111] The ex-employees claimed that their former employer unlawfully intercepted private and privileged telephone conversations by recording such conversations with a Dictaphone 9102 machine beginning in 1995. The Federal Circuit Court of Appeals affirmed a summary judgment for the employer, holding that the consent of one of the parties to a telephone conversation was not necessary to apply the ordinary course of business exception to the federal wiretapping provisions.[112] The *Arias* court also found that the alarm company's covert interception of employee telephone calls fell within the ordinary course of business exception.

In *Arias,* the secret surveillance by the employer was detected during a period in which there was a proposed sexual harassment settlement

---

104. *Id.*
105. 250 F.3d 980 (6th Cir. 2001).
106. *Id.* at 984.
107. *Id.*
108. *Id.* (citing Amati v. City of Woodstock, 176 F.3d 952, 955 (7th Cir. 1999)).
109. *Adams*, 250 F.3d at 984.
110. Nos. 96 Civ. 8447(LAK) & 96 Civ. 8448 (LAK), 1998 U.S. Dist. LEXIS 14414 (S.D.N.Y., Sept. 11, 1998).
111. *Id.* at *1; *see* Federal Wiretap Act (Title III), 18 U.S.C. § 2511 (2000).
112. Arias v. Mut. Cent. Alarm Serv., 202 F.3d 553 (2d Cir. 2000).

between a former and a current employee. In addition, there were pending divorce proceedings between the current employee and the owner's granddaughter.[113] The employer began to suspect that his employee was initiating divorce proceedings against his granddaughter and having an affair with a co-employee. During this period, the employees learned that the company was continuously recording the telephone conversations of all of its employees on a 24/7 basis.[114] In *Arias*, one of the plaintiffs overheard officers of the company listening to recordings of telephone calls. The court held that these calls arose in the ordinary course of business, because the owner had a legitimate ground for his suspicion that his current employee was disloyal.[115] The *Arias* court found that the alarm company had legitimate business reasons to "support the continual recording of all incoming and outgoing telephone calls."[116] The court reasoned that the alarm company was the repository of "extremely sensitive security information, including information that could facilitate access to their customers' premises."[117] The *Arias* court's definition of what was included in the ordinary course of business exception was so broad that it even included surveillance of conversations about personal relationships at the company.

Courts have had little difficulty extending the Federal Wiretap Act to e-mail and Internet communications as well as to telephone conversations. In *Konop v. Hawaiian Airlines, Inc.*,[118] a pilot sued his employer charging that the airline had viewed his secure website. The Hawaiian Airlines pilot "created and maintained a website where he posted bulletins critical of his employer, its officers, and the incumbent union, Air Line Pilots

---

113. The federal appeals court described the workplace as ensnared in a web of personal interconnections in the alarm company's workplace:

> There are a series of somewhat convoluted personal relationships between the parties, which are not directly relevant to the issues raised in this appeal. In the course of a dispute between [sexual harassment plaintiff] and [company officers] following her resignation in August 1995, [employer] began to suspect that [an employee], who was involved in divorce proceedings with [the officer's granddaughter] and was having an affair with [plaintiff], was a faithless employee. It was during this time that [the co-employees] allegedly first became aware that [the alarm company and its officers] had been continually recording the telephone conversations of all its employees, including theirs.

Arias, 202 F.3d at 555 (citations omitted).

114. *Id.* at 559.

115. The other set of phone calls conveyed a long-term affair between the former and the current employee, but also confidential discussions with an attorney about the divorce. These calls were seen as of personal nature and did not necessarily arise in the ordinary course of business.

116. *Arias*, 202 F.3d 559.

117. *Id.*

118. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. filed Aug. 23, 2002).

Association."[119] Other pilots employed by the airline permitted the airline's vice president to use their log-in information to establish accounts and passwords to log in to access the website.[120]

Later that day, the pilot received word that the Hawaiian Airlines vice president was upset by the contents of his website.[121] The pilot then became aware that the Airline's vice president had unauthorized access to his site,[122] and believed that the company official "had obtained the contents of his website and was threatening to sue [him] for defamation based on statements contained on the website."[123] The district court entered judgment against the pilot on his Federal Wiretap Act claim. The Ninth Circuit affirmed the lower court's ruling that the airline did not violate the Wiretap Act because the pilot's website was not intercepted during transmission, but rather while it was in electronic storage.[124] However, the court found that the airline violated the Stored Communications Act[125] because the two pilots who shared their log-in information were not "users" of the website at the time they authorized the airline officer to use their names.[126]

b. Title II of ECPA – Stored Communications Act (SCA)[127]

Once an e-mail is received and stored in the system it falls under the Stored Communications Act (SCA), or Title II, regardless of how temporary the storage.[128] Title II protects stored communications from unauthorized or exceeded authorized access, but it does not apply to the person or entities providing the wire or electronic communications service.[129] Further, it does not apply to the user of that service or in a

119. *Id.* at 872.
120. *Id.* at 873.
121. *Id.*
122. *Id.* at 873.
123. *Id.*
124. *Id.* at 878.
125. Electronic Communications Storage (Stored Communications) Act, 18 U.S.C. §§ 2701–2711 (2000).
126. *Id.* at 875.
127. 18 U.S.C. §§ 2701–2711 (2000).
128. The SCA states that it is a violation for anyone who "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 while it is in electronic storage in such system." 18 U.S.C. § 2701(a). "Electronic storage" is defined as (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication. 18 U.S.C. § 2510(17), 2711(1).
129. 18 U.S.C. § 2701(a), (c).

situation where the service was intended for that user.[130] This would, in many cases, authorize employers to monitor e-mails, since employers often provide the electronic communication service for their employees and the service is intended to be used within the scope of employment.

In *Bohach v. City of Reno*,[131] two police officers who were the subject of an internal investigation by the city sought an injunction to prevent disclosure of the contents of electronic messages sent between plaintiffs, pursuant to the ECPA.[132] The court held that the police department could retrieve pager text messages saved on the department's computer system without violating Title II of the ECPA or the privacy rights of the officers.

The court reasoned that the department was "'the provider' of the 'electronic communications service'" and "service providers [may] do as they wish when it comes to accessing communications in electronic storage."[133] The court classified stored transmissions of a paging system as storage irrespective of whether the storage of paging messages was classifiable as temporary, intermediate, or mere incidental "to its impending 'electronic transmission,' or more permanent storage for backup purposes."[134] The *Bohach* court found that there was no ECPA violation since the city government provided its personnel with the computers and software in order to give them the ability to send or receive electronic communications, and that the government could access or retrieve stored communications at their discretion.

The Third Circuit reasoned similarly in legitimating the retrieval of stored communications in *Frasier v. Nationwide Mut. Ins. Co.*[135] In *Frasier*, the Court of Appeals affirmed a grant of summary judgment in favor of the insurer on his ex-agent's wrongful termination claim, his

---

130. 18 U.S.C. § 2701(c)(1).

131. 932 F. Supp. 1232 (D. Nev. 1996).

132. The text pager system used by the police department functions by allowing a user to connect to a

> computer terminal and . . . then select[], from a list of all persons to whom pagers have been issued, the name of the person to whom the message is to be sent. The user then types the message and hits the 'send' key. The message is sent to the computer system's 'Inforad Message Directory,' where it is stored in a server file, and the user receives a message on the computer screen indicating that the page is being processed. The computer then dials the commercial paging company, sends the message to the company by modem, and disconnects. The user receives a 'page sent' message on the computer screen, and the paging company takes over, sending the message to the recipient pager by radio broadcast.

Id. at 1234.

133. *Id.* at 1236.

134. *Id.*

135. 352 F.3d 107 (3d Cir. 2003).

ECPA and parallel state claims, as well as his bad faith termination claim. The *Frasier* court rejected these claims following the *Bohach* court's literal interpretation of section 2701(c) that excepted "from Title II's protection all searches by communications service providers."[136]

The nature of e-mail systems makes it possible to copy a message several times during transmission and automatically store it on an employer's back-up system for later searches. This means that e-mails, according to current U.S. law, are normally considered stored communications, and employers are therefore authorized to access e-mails under this Title. This interpretation basically makes Title I useless to employees in protecting e-mails against prying employers.

c. The Law of Employer Surveillance Law

Justice Harlan explained that the Fourth Amendment protects people, not places, in his famous concurring opinion in *Katz v. United States*.[137] The basic methodology to determine what is a reasonable expectation of privacy balances facts against interests and values. Employers' control of their workplaces, such as searching lockers, monitoring phone calls, or video surveillance, has traditionally been the subject of intrusion upon seclusion claims by plaintiffs.[138] However, American courts have given employers the right to monitor in virtually every case decided over the last decade and have held that employees have no expectation of privacy in their electronic communications at work. Employers have successfully defended against common law and statutory claims by employees. Courts have only been receptive to privacy claims in the workplace in exceptional circumstances where the employer is prying into intensely private matters.

This section is followed by cases in which the company failed to implement a clear-cut policy about monitoring of employees' Internet or e-mail usage. Courts have had little difficulty finding that employees had no expectation of privacy where their employers provided them advance notice of monitoring, no matter how unclear, so long as the employee consented in advance to electronic surveillance. American courts have gone further and validated employers' right to monitor electronic communications, even when employees have received no advance warning about the employers' electronic surveillance.

---

136. *Id.* at 115.

137. 389 U.S. 347 (1967).

138. In order to establish a claim for intrusion upon seclusion, a plaintiff must prove: "(1) an intentional intrusion, physical or otherwise, (2) upon the plaintiff's solitude or seclusion or private affairs or concerns, (3) which would be highly offensive to a reasonable person." Mauri v. Smith, 929 P.2d 307, 310 (Or. 1996).

i. Employee Monitoring Without Notice

When companies began monitoring their employees' e-mail or Internet usage in the early to mid-1990s, relatively few companies had formal monitoring policies. Courts 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. These courts upheld e-mail spying as an acceptable employment practice and ignored Justice Hugo Black's admonition against secret surveillance:

> The average man would very likely not have his feelings soothed any more by having his property seized openly than by having it seized privately and by stealth. . . . And a person can be just as much, if not more, irritated, annoyed and injured by an unceremonious public arrest by a policeman as he is by a seizure in the privacy of his office or home.[139]

In *Restuccia v. Burk Technology, Inc.*,[140] the employer had no e-mail policy informing employees that their messages could be monitored or stored on a backup computer, or that there were any restrictions on personal messages except against "excessive chatting."[141] Employees were reminded to change their passwords frequently, but were not told that the supervisors had access to them.[142] In *Restuccia*, two ex-employees were terminated after their employer read their personal e-mail messages, which he had discovered while reviewing automatic backup-files.[143] The president of the company had used his supervisory password to gain access to the back-up files, where he learned that the employees had nicknames for him.[144] He discovered e-mails making reference to his own extramarital affair with another company employee.[145] During one of the employees' performance reviews, the president told him he was spending too much time using the e-mail system.[146] Later, the president terminated the employees on the personal grounds that they were using the system too much, without reference to the fact that they were gossiping about his extramarital affair.[147]

---

139. Griswold v. Connecticut, 381 U.S. 479, 509 (Black, J., dissenting).
140. No. 95-2125, 1996 Mass. Super. LEXIS 367 (Mass. Super. Aug. 13, 1996).
141. *Id.* at *2.
142. *Id.*
143. *Id.* at *3.
144. *Id.*
145. *Id.*
146. *Id.*
147. *Id.*

The ex-employees filed suit alleging multiple claims, including the invasion of privacy.[148] The plaintiffs argued that they had an expectation of privacy in these e-mails because they had personal passwords to access the message program.[149] The court found "genuine issues of material fact on the issue of whether plaintiffs had a reasonable expectation of privacy" in stored employees' e-mails and that there was a question of whether the president's reading of e-mail messages on its back-up system "constituted an unreasonable, substantial or serious interference with plaintiffs' privacy."[150] The court also refused to enter summary judgment in favor of the corporate defendant on their tort-based claims for wrongful termination, negligent infliction of emotional distress and loss of consortium.[151] The *Burk* case was a plaintiff victory in that the court acknowledged the possibility of a plaintiff receiving redress in a workplace interception case. In every other private workplace case up to that point, the defendant had been awarded summary judgment on claims that workplace electronic surveillance invaded a plaintiff's right of privacy.

In *Smyth v. Pillsbury Co.*,[152] the court found no expectation of privacy when an employer intercepted private e-mails after giving all employees notice that it was monitoring electronic communications. In *Smyth,* an employer fired an employee after intercepting private e-mail messages that made disparaging comments about the sales management. The e-mails from the terminated employee concerned sales management and "contained threats to 'kill the backstabbing bastards' and referred to the planned Holiday party as the 'Jim Jones Kool-Aid affair.'"[153] The company had "repeatedly assured its employees, including [the] plaintiff that all e-mail communications would remain confidential and privileged."[154] Soon after the employer intercepted the plaintiff's e-mails, the company president terminated his employment on the grounds that he was "transmitting what it deemed to be inappropriate and unprofessional comments over [the company's] e-mail system."[155]

The at-will employee claimed that he was wrongfully terminated in violation of "public policy which precludes an employer from terminating an employee in violation of the employee's right to privacy."[156] The federal court upheld the employer's termination, ruling that there was no public policy exception since the employee had no expectation of privacy

148. *Id.*
149. *Id.* at *8.
150. *Id.* at *9.
151. *Id.* at *11.
152. 914 F. Supp. 97 (E.D. Pa. 1996).
153. *Id.* at 99.
154. *Id.* at 98.
155. *Id.* at 98–99 (citations omitted).
156. *Id.* at 100.

in the employer's e-mail system.[157] The court also rejected the ex-employee's claim that the employer's interception of his e-mail intruded upon his seclusion, stating that the employee could not have a reasonable expectation of privacy in e-mail communications voluntarily made over the company e-mail system.[158] The court went even further, positing that even if the employee had a reasonable expectation of privacy in the contents of his e-mail communications over the company e-mail system, it would not be a highly offensive invasion of privacy if his employer intercepted messages on a system that it owned.[159] The court observed that the company's interception of the employee's e-mail messages was justified because the company had a substantial interest in preventing inappropriate and unprofessional comments over its e-mail system, which outweighed any privacy interests that the employees might have in their e-mail communications.[160]

In *McLaren v. Microsoft Corp.*,[161] an employee charged Microsoft with invading his reasonable expectation of privacy when it accessed his personal folders on a network that allowed storage of e-mail messages in order to further an internal investigation of sexual harassment and inventory shortages.[162] The plaintiff filed suit against Microsoft charging that the company invaded his privacy by "breaking into" some or all of the personal folders maintained on his office computer and releasing the contents of the folders to third parties.[163] Microsoft's ex-employee claimed that he had an expectation of privacy when Microsoft allowed him to store a "password for his personal folders."[164] The plaintiff in *McLaren* characterized Microsoft's decrypting or otherwise "breaking in" to his personal folders as an intentional, unjustified, and unlawful invasion of privacy. In that case, Microsoft gained access to the plaintiff's communications through a network password as well as a personal password created by the plaintiff and authorized by Microsoft. The company uncovered e-mail evidence that the plaintiff was engaging in a systematic pattern of sexual harassment.[165] Microsoft reviewed and disseminated electronic mail stored in a "personal folder" on the employee's office computer.[166] The *McLaren* court did not recognize a cause of action for invasion of privacy even if the employee had a special

157. *Id.* at 101.
158. *Id.*
159. *Id.*
160. *Id.*
161. No. 05–97–00824–CV, 1999 Tex. App. LEXIS 4103 (Tex. App. 1999).
162. *Id.* at *2.
163. *Id.*
164. *Id.* at *1.
165. *Id.* at *3.
166. *Id.*

password and marked the files "personal," since the computer was the property of the employer and only a part of the office environment.[167] The court also stated that the e-mail messages stored in the plaintiff's personal folder had been transmitted over the network and had become accessible to a third party at some point. Therefore, the plaintiff had no expectation of privacy in those files even if he marked them as private.[168]

The *McLaren* court distinguished a private e-mail folder from a search of a locker where there was an expectation of privacy.[169] The court reasoned that an employee was issued a locker with the specific purpose of storing personal belongings, whereas the plaintiff's computer was provided solely for employment-related reasons.[170] The court noted:

> Even [if the plaintiff's practice was to move e-mail messages to personal folders], any e-mail messages stored in McLaren's personal folders were first transmitted over the network and were at some point accessible by a third-party [because they were temporarily stored in the central routing computer accessible to the employer]. Given these circumstances, we cannot conclude that McLaren, even by creating a personal password, manifested—and Microsoft recognized—a reasonable expectation of privacy in the contents of the e-mail messages such that Microsoft was precluded from reviewing the messages.[171]

The court hypothesized that even if it were to conclude that the plaintiff had an expectation of privacy in his company's e-mail system, a reasonable person would not find an interception of e-mail to be highly offensive, and therefore there could be no intrusion upon seclusion.[172]

ii. Notice-Based Electronic Monitoring

Employers have increasingly implemented e-mail and Internet usage policies to protect their intangible assets and to reduce their exposure to

---

167. *Id.* at *4.
168. *Id.*
169. *Id.* at *3.
170. *Id.*
171. *Id.* at *4 (citations omitted).
172. Even if we were to conclude that McLaren alleged facts in his petition which, if found to be true, would establish some reasonable expectation of privacy in the contents of his e-mail messages sent over the company e-mail system, our result would be the same. We would nevertheless conclude that, from the facts alleged in the petition, a reasonable person would not consider Microsoft's interception of these communications to be a highly offensive invasion.

Id. at *5.

litigation. An empirical study found that seventy-nine percent of employers implemented a written e-mail policy by 2004, up slightly from seventy-five percent in 2003.[173] Employers were less vigilant in including training modules for e-mail or Internet usage. Of those companies with an e-mail or Internet usage policy, only fifty-four percent provided training regarding the implications of violating the policy.[174]

When a company implements an e-mail or Internet policy, it virtually eliminates any privacy-based claim by employees who are the target of monitoring electronic communications. In *Bourke v. Nissan Motor Corp.*,[175] for example, the employees signed a waiver form which required them to acknowledge their understanding that Nissan's e-mail policy was to restrict the use of e-mail to business purposes. The *Nissan* court found that the company's waiver form was fatal to the employees' claims that the company invaded their privacy by intercepting e-mail messages which had a salacious content. The court also held that the plaintiffs were aware that co-workers could read their e-mails and that the company had a right, as a system operator, to access the network.

In *Garrity v. John Hancock Mutual Life Insurance Co.*,[176] two long-time employees of the insurance company were terminated after forwarding sexually explicit e-mails from Internet joke websites and from other third parties.[177] One of their co-employees complained to management after receiving a forwarded e-mail from the plaintiffs.[178] John Hancock promptly commenced an investigation of the plaintiffs' e-mail folders, as well as the folders of those with whom the plaintiffs e-mailed on a regular basis. The court found that the e-mail violated the insurer's e-mail policy which prohibited "[m]essages that are defamatory, abusive, obscene, profane, sexually oriented, threatening or racially offensive."[179]

The terminated women contended that the insurer's "e-mail policy is almost impossible to locate on Hancock's intranet system, and even harder to decipher."[180] They also argued that the reminders the insurer sent "did

173. American Management Association, *2004 Workplace E-Mail and Instant Messaging Survey* (2004), *available at* http://www.amanet.org/research/pdfs/IM_2004_Summary.pdf; American Management Association, *2003 E-mail Rules, Policies and Practices Survey* (2003), *available at* http://www.amanet.org/research/pdfs/Email_Policies_Practices.pdf.

174. *Id.*

175. No. B068705 (Cal. Ct. App. July 26, 1993), *available at* http://www.law.seattleu.edu/fachome/chonm/Cases/bourke.html.

176. No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343 (D. Mass. May 7, 2002).

177. *Id.* at *1.

178. *Id.* at *2.

179. *Id.*

180. *Id.*

not accurately communicate its e-mail policy."[181] The ex-employees disputed the insurer's characterization of the e-mails in question as sexually explicit or in any way in violation of the policy language. Upon review of the e-mails in question, however, the court found that the e-mails were sexually explicit within the meaning of defendant's e-mail policy. Regardless, the plaintiffs asserted that Hancock led them to believe that these personal e-mails could be kept private with the use of personal passwords and e-mail folders.[182]

The *John Hancock* court dismissed the plaintiff's privacy-based actions since they had no reasonable expectation of privacy in e-mails transmitted on their employer's computer system. The court relied on *Pillsbury* and concluded that an employee does not have any expectation of privacy in his work e-mail, since the expectation is lost as soon as the employee voluntarily uses an e-mail account provided at work. Whether the company has an e-mail policy is of no importance. Further, the court stated that the interest of the employer to take affirmative steps against harassment is more important than the plaintiff's privacy interest.

In *Thygeson v. U.S. Bancorp,*[183] a federal magistrate reiterated the conventional wisdom that employees have no reasonable expectation of privacy in computers owned by a company. In *Thygeson,* an employee with over eighteen years of service with the bank was terminated without severance benefits for violating the company's policy regarding inappropriate use of the Internet. The company's employment handbook stated only that employees were not to "use U.S. Bancorp computer resources for personal business."[184] Another statement in the defendant's employee handbook warned: "Do not access inappropriate Internet sites and do not send e-mails which may be perceived as offensive, intimidating, or hostile or that are in violation of Company policy."[185] U.S. Bancorp reserved the right "to monitor any employee's e-mail and computer files for any legitimate business reason, including when there is a reasonable suspicion that employee use of these systems violates" the company's Internet policy.[186]

The company estimated that the terminated employee, who had no work-related reason to visit Internet sites, was spending more than four hours per day visiting websites on his work computer.[187] The bank uncovered "inappropriate e-mails containing pictures of nudity and

181. *Id.* at *3.
182. *Id.*
183. No. CV-03-467-ST, 2004 U.S. Dist. LEXIS 18863 (D. Or. Sept. 15, 2004).
184. *Id.* at *14.
185. *Id.*
186. *Id.* at *14–15.
187. *Id.* at *9.

sexually offensive jokes" saved on the company's computer system.[188] The plaintiff was terminated and he filed claims for the invasion of privacy as well as under the federal Employee Retirement Income Security Act (ERISA), given that he was fired without severance benefits.[189]

He predicated this claim on the fact that other individuals misused the computer system and were not terminated, and argued that the company was looking for a reason to fire him for "cause."[190] The court ruled that the plaintiff's ERISA claim was barred due to his failure to exhaust administrative remedies.[191] The court entered summary judgment against the plaintiff on his invasion of privacy claim, ruling that he had no expectation of privacy when the company accessed "files he stored in his 'personal' folder of U.S. Bancorp's computer network and remotely determine[ed] the address of the websites he visited while at work."[192] The court found the employee's personal messages saved on the company's computer to be unprotected, just as in the *McLaren* case.[193] The court observed that if the plaintiff in *McLaren* had no expectation of privacy when his employer accessed the files on its network that the plaintiff had saved using a personal password, then this employee had no expectation of privacy in his e-mail which he "merely labeled 'personal' without even creating a password."[194]

The path of Internet privacy law forged by U.S. courts has a decidedly pro-employers spin, leaving employees without meaningful remedies for employer abuses of electronic e-mail and Internet surveillance. As we have seen, nearly every court has held that American employees have no right of privacy in the electronic workplace. The U.S. courts' mechanical jurisprudence is based upon a theory of property rights, which reasons that since business computers are the property of the employers, employers have an unfettered right to monitor usage. The employers' unfettered right to monitor gives employers the perverse incentive to pretextually terminate employees to save the money from paying retirement or severance benefits.

In the *John Hancock* case, for example, the plaintiffs were near retirement age and it is questionable whether forwarding e-mail jokes was an offense so serious as to justify termination. Plaintiffs will not find relief under the U.S. Constitution, the common law of torts, or the ECPA. At present, workers have no means to moderate the harsh effects of abusive workplace monitoring practices. In the next part, we explain how U.S.

188. *Id.*
189. *Id.* at *2.
190. *Id.* at *18.
191. *Id.* at *59.
192. *Id.* at *60.
193. *Id.* at *63.
194. *Id.* at *65.

workers are affected by not having any meaningful remedies against workplace monitoring by contrasting our market-driven property approach to the well-established European tradition of regarding privacy as a fundamental right.

III. WORKPLACE PRIVACY AS A HUMAN RIGHT: THE EUROPEAN APPROACH

> We live in a virtual world where the global transmission of information is becoming almost seamless. The operations of governments and corporations are profoundly transformed by the emergence of e-government and e-commerce. Electronic collection, use, sharing and storage of personal information is at the hub of this transformation which modifies not only the way organizations carry out their daily business but also, more fundamentally, the manner by which they communicate with citizens, consumers, clients and stakeholders.[195]

Privacy in the United States does not enjoy the same exalted status as free speech and the right to vote. In the nineteenth century factory, "monitoring took the unsophisticated form of a supervisor walking the assembly line and visually inspecting employee work."[196] Today's more sophisticated electronic tracking of employees' Internet and e-mail use diminishes privacy even further in the workplace. "Many fear that the new danger of the technological workplace is the 'electronic sweatshop' where employees are subject to constant electronic monitoring."[197] While there is no constitutional right of privacy in the private sector workplace, the law is not settled until it is settled right.[198]

---

195. Jennifer Stoddart, Privacy Commissioner of Canada, Submission of the Office of the Privacy Commissioner of Canada to the Office of the Information and Privacy Commissioner for British Columbia, Pike & Fischer's Internet Law & Regulation 2004 ILRWeb (P&F) 2429 (Aug. 18, 2004), *available at* http://Internetlaw.pf.com/fulldoc1.asp?iDoc=2&section=1&referrer=advsearch.asp (last visited May 4, 2005).

196. Jarrod D. White, *E-mail@Work.com: Employer Monitoring of Employee E-Mail*, 48 ALA. L. REV. 1079, 1079 (1997) ("Despite its arduous development, the net result of this process was a somewhat straightforward understanding by employers and employees of their legal rights concerning privacy in the workplace. However, emerging technology at the sunset of the twentieth century, particularly the pervasive use of electronic mail (E-mail) by private sector companies, has unleashed new uncertainty concerning privacy rights in the workplace.").

197. Eric M.D. Zion, *Protecting the E-Marketplace of Ideas by Protecting Employers: Immunity for Employers Under Section 230 of the Communications Decency Act*, 54 FED. COM. L.J. 493, 512 (2002).

198. It was once conventional wisdom that the Fourth Amendment was not violated when telephone surveillance was conducted since there was no physical penetration of the

In F. Scott Fitzgerald's famous book *The Great Gatsby*, the author writes about a green mysterious light that is later symbolized as the American dream where visionaries and explorers could hope for a better future when first entering the ground in New England.[199] Today that green light could be seen as the dream about the technological revolution, and the faith in Internet and electronic communications. The main character in *The Great Gatsby* loses all hope in the end and believes that humans are unable to move beyond the past, and that the green light as a symbol for hope has devolved into a pursuit of wealth.[200] Now, after the first exploration of the virtual world has been completed, we need to strike some balance in order to keep the dream about the World Wide Web alive and not turn it into a shallow and empty shell. Therefore, employers need to be able to monitor their employees, like the eyes of Dr. Eckleberg, but in a less intrusive way, with limitations on the right of employers to monitor electronic communication systems in order to safeguard corporate assets. Employers in America should be required to inform employees of electronic surveillance, obtain their consent, and formulate clear e-mail and Internet policies. Employees might once more "rage against the machine," as during the Industrial Revolution in England, resulting in original resistance.[201] Therefore, there is a need for American employers to recognize at least a minimum right of privacy with respect to their employees.

Privacy has been regarded as a fundamental right throughout Europe since the middle of the Eighteenth Century. Americans have little by way of statutory protection for privacy outside of a few sectors, such as health care and financial services. Europeans find the U.S. approach to privacy too amorphous, lacking the focus or saliency of this value in its legal system and culture.

This Part of the Article will demonstrate that the European employees of PhDog.com have an unqualified right to be given notice of their employer's monitoring practices, and that any use of information obtained by electronic surveillance is illegal without such notification. If PhDog applied the same policies in their French subsidiary as they have implemented in the United States, 175 executives would face civil and criminal liability, with the prospect of prison time and fines. In addition,

---

telephone booth. Olmstead v. United States, 277 U.S. 438 (1928). The Court reversed course, ruling that the Fourth Amendment was not foreclosed by the interception of electronic communications. Katz v. United States, 389 U.S. 347 (1967) (holding that warrantless wiretapping violated the Fourth Amendment).

199. FITZGERALD, *supra* note 7, chs. 1 & 9.

200. *Id.*

201. *See* Luddites—The Machine Breakers, Cotton Times (recounting Luddites breaking the "Spinning Jenny" during the Industrial Revolution), *available at* http://www.cottontimes.co.uk/luddo.htm (last visited May 28, 2005) .

the firm would face lawsuits by the government, as well as by employees monitored without notice. In order to explain this great disparity between American and European employment law, we will trace the evolution of privacy as a human right in Europe. We first will anchor the development of privacy as a fundamental right through a brief sketch of this legal norm's evolution beginning with the Enlightenment and continuing through Europe's Industrial Revolution to the post-modern period.

The European workers' right to privacy is inextricably linked with the development of trade unions, worker self-control, and self-determination. As a result of this history, the predominant labor law issue is consultation with trade unions, elected employee representatives, and greater democracy through work councils.[202] The greater value placed on workplace privacy by Europeans stems from Europe's history of recognizing worker self-determination. The contrasting approaches taken in Europe and the United States can largely be explained by the Americans' "peculiar attachment to the notion of 'employment-at-will'"[203] which is the idea of "employer sovereignty" and which diverges markedly from the European tradition.

Next, we will examine the two different administrative bodies dealing with privacy protection as a fundamental right in Europe. First, we look at the role of the Council of Europe in ensuring fundamental human rights, including the right to privacy to one's life and correspondence. The Council of Europe, based in Strasbourg, France, is a transnational political institution created in 1949 to promote greater unity among its member states. Today the Council seeks to protect human rights and democracy, to foster peace among the forty-six member states, and to develop a common response to political, social, cultural, and legal challenges.[204]

During the past fifty-five years, the Council has evolved from an advocate of human rights to a watchdog that also provides information and assistance to support the original aims of the Council. The rules and the case law developed through the Convention on Fundamental Human Rights by the European Council form the basis for the European Union's legislation on data protection and privacy.[205] Next, we will examine the role of the European Union's directives as they relate to electronic surveillance of employees in the workplace.

Directives must be implemented in each member state's national law

---

202. FRASIER YOUNSON, CROSS-BORDER REDUNDANCIES, GLOBAL COUNSEL LABOUR & EMPLOYEE HANDBOOK 341 (2002).

203. Eltis, *supra* note 18, at 490–91.

204. At present, the Council of Europe is composed of forty-six member states, half of whom are also members of the European Union. Council of Europe, *About the Council of Europe* (Jan. 2005), *at* http://www.coe.int/T/e/Com/about_coe/.

205. European Commission, *Privacy Protection*, *at* http:// europa.eu.int/information_ society/topics/ecomm/all_about/todays_framework/privacy_protection/index_en.htm (last updated May 24, 2005).

and are more specific than the American standard-based approach discussed in Part I of this Article. The European Data Protective Directive, for example, creates uniformity of member states' protection of privacy for Europeans by imposing standards for processing personal information.[206] The European Community is in the process of drafting a new Directive specifically aimed at a "right to protection of personal data,"[207] building on the protections already in place under the European Union Data Protection Directive and providing greater specific protection for privacy in the employment context.

Finally, we will examine the privacy-based legislation of the United Kingdom and France, which has its roots in European Union developments. We will show that a multinational company with branches in America and Europe needs to understand both legal cultures in order to avoid criminal and civil liability when monitoring their employees.

A. The PhDog.com Branch in Europe

Our hypothetical PhDog, presented in Part I, faces the same kind of liability claims and concerns in France as in the United States, such as sexual harassment claims, preventing the loss of intellectual property, and productivity losses. However, while PhDog.com does not face any real civil or criminal liability claims from its American employees for abusive monitoring practices, it will be held to a heightened standard when it comes to its French employees. This is because, contrary to American law, French law requires employers to clearly inform employees that monitoring will take place and to show that the employees have actual notice of such monitoring. PhDog.com's management officers could face up to three years in prison and/or 45,000 Euro in fines in France for e-spying on the company's French employees.[208]

Further, PhDog.com's clandestine e-surveillance is a violation of French employees' human rights irrespective of whether the e-mails are

206. The data protection traditions varied significantly across member states. Germany, France, and United Kingdom had a tradition of strong protection of privacy versus non-existent regulation in Greece. RONALD J. MANN & JANE K. WINN, ELECTRONIC COMMERCE 187 (2002).

207. European Industrial Relations Observatory On-line, *New Technology and Respect for Privacy at the Workplace* 5, *available at* http://www.eiro.eurofound.eu.int/print/2003/07/study/tn0307101s.html (last visited May 29, 2005).

208. Nikon France v. Onos, Cass. Soc. Arret No. 41-6410/2/01 (France 2001); CODE DU TRAVAIL [C. TRAV.] art. L.121-8, R. 122-12 and L. 412-8 (Fr.), *available at* http://lexinter.net/Legislation5/forme_et_langue_du_contrat_de_travail.htm (last visited May 28, 2005); CODE PENAL [C. PEN.] art. 226-15 (Fr.), *available at* http://www.legifrance.gouv.fr/html/codes_traduits/code_penal_textan.htm (last visited May 28, 2005).

personal or work-related, and its officers could be haled into the European Court of Human Rights.[209] Additionally, even if PhDog were to articulate a clear e-mail and Internet usage policy that all private correspondence is forbidden, the French employees would still have the right to use the network for some personal use as well as store personal files on the computer, because the French legislation does not recognize a total ban as a proportional measure.[210]

All of this means that PhDog.com must treat its French employees differently than it treats its American employees. Moreover, whereas its American employees have no legally enforceable expectation of privacy in their e-mail or Internet usage, PhDog.com's monitoring policies for its French subsidiary's employees must be tailored to protect their privacy. In order to be able to advise an international company like PhDog.com, it is important to understand the reason for localizing monitoring policies. The next section will explain how the European human rights approach was developed and how it has evolved.

B. Protecting the Private Sphere of European Electronic Communications

When it comes to privacy, the United States and Europe have two different cultures. The differences between the two cultures can be seen in their different responses to homeland security. The U.S. is far more predisposed to subordinate privacy to security than the Europeans are. In November of 2004, a federal agency "ordered U.S. airlines to turn over names and other data on millions of passengers to assist tests of Secure Flight,"[211] an order that raised privacy concerns in Europe. Members of the European Parliament "warned the European Commission that unless it announces the withdrawal of the E.U.-US passenger data transfer agreement,"[212] the European Parliament would refer the matter to the European Court of Justice. Travelers from Europe must now submit to fingerprinting and photographs, and data on passenger information is exchanged with U.S. security officials.[213]

The U.S. approach to online privacy has largely focused on a self-

209. ECHR, Nov. 4, 1950, art. 8, 213 U.N.T.S. 221 [hereinafter ECHR], *available at* http://www.pfc.org.uk/legal/echrtext.htm.

210. CODE DU TRAVAIL [C. TRAV.] art. L.122-43 (Fr.). Nikon France v. Onos, Cass. Soc. Arret No. 41-6410/2/01 (France 2001).

211. John M. Doyle, *U.S., EU to Trade Information on Sensors, MANPADS Defense*, (Nov. 24, 2004), at 4, *available at* LEXIS, CURNWS Library.

212. Sharon Spiterii, *MEPS Give Commission Ultimatum on Data Transfer to U.S.*, EUObserver.com (Apr. 16, 2004), *available at* LEXIS, CURNWS Library.

213. Elizabeth Olson, *Screening Program Takes Hold in the U.S.*, INT'L HERALD TRIBUNE, Sept. 30, 2004, at 24.

regulatory or market-driven approach[214] as opposed to government enforcement. The federal government does not strictly scrutinize privacy except in selected sectors such as health care[215] and financial services.[216] In contrast, the European member states have been enacting national privacy laws to comply with the Data Protection Directive since October 1998. These enactments also have profound implications for the monitoring of Internet systems and networks. The European approach to Internet privacy is a "command and control" model with specific rules governing the handling of personal information, in contrast to the American approach of general standards that are chiefly market-driven. The European Union Directives have had an enormous impact on non-E.U. countries because we are living in a global economy where personal data crosses borders seamlessly. U.S. companies will be in violation of European human rights law by conducting electronic surveillance of European workers and transferring the results to countries like the United States that do not afford adequate privacy protection for employees' personally identifiable information.[217]

European countries have formulated an all-encompassing cultural and legal response to privacy-based actions as compared to the United States, which continues to delineate a sharp distinction between private and public workplaces.[218] Throughout Europe, privacy legislation applies equally well to public or private entities that collect and handle personal information. The protection of the individual has been a critical issue throughout Europe for several centuries because of the historical struggle to establish workers' rights. To understand the differences in privacy protections between Europe and the United States, it is necessary first to study historical antecedents of this fundamental value. As Justice Oliver Wendell Holmes notes well:

---

214. Our analysis of Federal Trade Commission cases shows that the FTC is stepping up its enforcement of online privacy. "If a web site has a privacy policy, but its information collection and use practices are inconsistent with that policy, the FTC has authority to investigate and restrain the misrepresentations in the privacy policy as unfair or deceptive trade practices. Kirk J. Nahra, *What Every Insurer Needs to Know About Privacy*, 5-21 MEALEY'S EMERG. INS. DISPS. 16 (2000).

215. The requirements of the Health Insurance Portability and Accounting Act (HIPAA) apply equally well to the Internet.

216. The requirements of the Gramm-Leach-Bliley Act focus on privacy protection for the individual customers of financial institutions. Nahra, *supra* note 214.

217. *See New.Technology and Respect for Privacy at the Workplace*, *supra* note 207.

218. The Federal Republic of Germany is emblematic of the greater protection given to privacy in Europe. "Germany has a scheme of integrated privacy and data protection laws at the federal and state levels, based on constitutional language and judicial decisions, that is a model for federal systems offering protection for personal privacy." David H. Flaherty, *On the Utility of Constitutional Rights to Privacy and Data Protection*, 41 CASE. W. RES. L. REV. 831, 841 (1991) (internal citations omitted).

> The law embodies the story of a nation's development through many centuries, and it cannot be dealt with as if it contained only the axioms and corollaries of a book of mathematics. In order to know what it is, we must know what it has been, and what it tends to become.[219]

In order to understand the European approach to electronic surveillance, it is important to understand the overriding value of freedom that can be traced all the way back to the French Revolution, when workers fought to be recognized as free individuals.[220] The French Revolution displaced feudal institutions, giving French citizens freedoms such as the right to contract in its calls for liberty, equality, and fraternity.[221]

In the next section we will show how the workers' rights movement first developed in Europe in order to explain the path of privacy law as a fundamental right. In Europe, the right to privacy and correspondence has been respected as a fundamental right for over fifty years and is still an important aspect of privacy protection for individuals. Europeans have far more developed privacy protections than the United States despite having vastly different "social mores, . . . countries, regions and people,"[222] and contend to maintain "unity in diversity."[223]

---

219. OLIVER WENDELL HOLMES, THE COMMON LAW 5 (2d ed. 1963).

220. On April 12, 1811, a decade or so after the French Revolution called for freedom, equality, and fraternity, Beethoven wrote the following note to Goethe, who authored the tragic story of Egmont, the nobleman who fought to liberate the Netherlands from Spain's political, economic, and religious oppression: "You will shortly receive . . . the music for Egmont; that glorious Egmont which through you I have considered, felt and set to music with the same warm emotions as I experienced when I read it."

Boris Kozolchyk, *NAFTA in the Grand and Small Scheme of Things*, 13 ARIZ. J. INT'L & COMP. LAW 135, 135 (1996) (citation omitted).

The first progress towards workers' rights in France came after the French Revolution, when France was transformed from an absolute monarchy to a republic where the citizenry theoretically received free and equal rights. The French Revolution was itself part of a workers' rights movement as the French people were dissatisfied with the grossly unfair tax system, persecution of religious minorities and the government's interference with their private life. The French Revolution, *available at* http://ap_history_online.tripod.com/apeh8.htm (last visited May 28, 2005).

221. Kozolchyk, *supra* note 220, at 136.

222. Nonnie L. Shivers, Note, *Firing 'Immoral' Public Employees: If Article 8 of the European Convention on Human Rights Protects Employee Privacy Rights, Then Why Can't We?*, 21 ARIZ. J. INT'L & COMP. L. 621, 654 (2004).

223. Europa, The European Union at a Glance, *at* http://www.europa.eu.int/abc/print_index_en.htm (last visited May 28, 2005).

1. The Rise of the Union Movement

> Here, then, is the "curse" of our factory-system; as improvements in machinery have gone on, the "avarice of masters" has prompted many to exact more labor from their hands than they were fitted by nature to perform, and those who have wished for the hours of labour to be less for all ages than the legislature would even yet sanction, have had no alternative but to conform more or less to the prevailing practice, or abandon the trade altogether.[224]

The American approach to electronic surveillance of employees may be traced to the view that employers enjoy an absolute sovereignty through property and contract. In contrast, Europeans have long viewed workplace privacy as a highly treasured value.[225] The rise of the workers' self-determination movement in Europe was prefigured by organized resistance to the horrors of early industrialization and its abhorrent factory system. The union movement is a direct response to the textile industry's conditions in England during the mid-1700s. Worker self-determination was not a significant issue prior to 1760 because the mechanical inventions that deskilled work had yet to be developed.[226]

No industrial development was as transformative as inventions such as the Flying Shuttle, The Spinning Jenny, and the Water Frame.[227] England was soon to be in the throes of social change, spearheaded by the development of the Spinning Jenny by James Hargreaves in 1764.[228] Mr. Hargreaves established a spinning business in Nottingham, leaving his native Lancashire fearful of that city's hostility to the novel technology.[229]

---

224. John Fielden, *The Curse of The Factory System* 34–35 (1836), *available at* http://www.victorianweb.org/history/workers2.html (last visited May 28, 2005).

225. *See* Eltis, *supra* note 18 (explaining the employer sovereignty approach to electronic surveillance and comparing the American legal system's emphasis on contract and property to fundamental human rights).

226. ARNOLD TOYNBEE, LECTURES ON THE INDUSTRIAL REVOLUTION IN ENGLAND (1884), *available at* http://socserv2.socsci.mcmaster.ca/~econ/ugcm/3ll3/toynbee/indrev (last visited May 28, 2005).

227. At first, however, the absorption of the small freeholders went on slowly. The process of disappearance has been continuous from about 1700 to the present day, but it is not true to say, as Karl Marx does, that the yeomanry had disappeared by the middle of the eighteenth century. It was not till the very period, which we are considering, that is to say about 1760, that the process of extinction became rapid. *Id. See generally* E. P. THOMPSON, THE MAKING OF THE ENGLISH WORKING CLASS (1963); *see also* E. P. THOMPSON, WHIGS & HUNTERS (1975).

228. This was the first weaving machine that allowed one person to spin many threads at once and was an improvement of John Key's first "flying shuttle" from 1733. The Industrial Revolution, Innovations of the Industrial Revolution, *at* http://industrialrevolution.sea.ca/innovations.html (last updated Feb. 17, 2003).

229. Luddites—The Machine Breakers, *supra* note 201.

The widespread adoption of the "Spinning Jenny" in the textile industry displaced the traditional hand-loom weavers and other artisans.[230] In 1811 textile manufacturers in Nottingham received letters signed by "General Ned Ludd and his Army of Redressers."[231] The Luddites raged against the machines of production to protect their jobs. E.P. Thompson, the eminent English historian, contended that the Luddite saboteurs were more than machine-smashers, but that they represented a social movement against the factory system and the price system that constituted the new economic order of capitalism.[232]

William Pitt, the British Prime Minister, convinced Parliament to enact laws in 1780 and later in 1799 to stave off the "political agitation among industrial workers."[233] Taking advantage of public panic about the mushrooming unionist movement, many employers moved to crush all labor organizations. The British Parliament enacted the so-called "Combination Laws," "making it illegal for workers to join together to press their employers for shorter hours or may [sic] pay. As a result trade unions were thus effectively made illegal."[234] However, in reality the Combination Acts were unable to prevent workers from organizing unions and attending clandestine meetings.[235] Despite the legal backlash against

---

230. E. P. THOMPSON, THE MAKING OF THE ENGLISH WORKING CLASS 3 (1963).

231. "Ludd probably did not exist, although there is some suggestion that the name was derived from that of a Leicestershire farm labourer who had destroyed some stocking frames about 1782." Luddites—The Machine Breakers, *supra* note 201.

232. *See generally* E.P. THOMPSON, THE MAKING OF THE ENGLISH CLASS (1963).

> And by 1850, England had become an economic titan. Its goal was to supply two-thirds of the globe with cotton spun, dyed, and woven in the industrial centers of northern England. England proudly proclaimed itself to be the 'Workshop of the World.' Thomas Carlyle described the emergence of a 'cash nexus,' where the only connection between men is the one of money, profit and gain.

The History Guide, *Lectures on Modern European Intellectual History, The Origin of the Industrial Revolution in England* (Lecture 17), *at* http://www.historyguide.org/intellect/lecture17a.html (last revised May 13, 2004).

233. *Combination Acts*, *at* http://www.spartacus.schoolnet.co.uk/Lcombination.htm (last visited May 28, 2005).

234. *Id.*

235. *Id.* Parliament reversed course only twenty-four years later legitimating trade unions. *Sheffield Trade Outrage*, *at* http://www.shef.ac.uk/misc/personal/cm1djw/lochist/outrage1.htm (last visited May 28, 2005). Robert Owen created the Grand National Consolidated Trade Union in 1834, the largest and most visionary early national union at that time, which skyrocketed in membership to over a half million workers within a few weeks. To join the Grand Union, workers paid an entrance fee of one shilling and swore an oath during an initiation ceremony. In Dorset village of Tolpuddle there was an act forbidding illegal oaths. Under this law six men were found guilty and deported to Australia for seven years. These workers became known as the Tolpuddle Martyrs. However, the "Grand National" was not able to maintain its speedy growth and declined rapidly because

unions by the government, unions were well established by 1850 and gradually became more effective in their strategies to improve working conditions, raise wages, and improve bargaining power. By 1868, workers formed the first Trade Unions Congress and introduced the Trade Unions Act of 1871.[236]

If we fast forward to the new millennium, we see tremendous strides in workers' rights throughout Europe. This brief synoptic sketch traces the long struggle for workers' rights that continues to this very day with improving privacy protections in the electronic workplace. While there is no more rage against machines of production to protect jobs today, European workers are keenly aware of their rights that were won through centuries of struggle. Today, electronic surveillance is the functional equivalent of the industrial sweatshop of the Eighteenth Century. Modern employees have information-based concerns, such as how to protect their private lives in order to prevent their workplace from devolving into electronic sweatshops. Even if those rights are protected as fundamental human rights in Europe, there is uncertainty as to how privacy can be protected against corporate and governmental Big Brothers. The path of European law has been to balance workers' right to privacy against the need to protect corporate assets, interests, and rights. The legislation from the European Council and the European Union reflects a continuing need to update and modernize fundamental rights in the modern workplace.

2. Efforts by the Council of Europe

The Council of Europe was created after World War II as a transnational political institution with the aim of protecting human rights and democracy and fostering peace among its forty-six member states.[237] The Council of Europe is not a legal institution of the European Community, even though its legislative decrees may be binding upon most of the European countries.[238] The Convention for the Protection of Human Rights and Fundamental Freedoms of 1950, which is enforced by the European Court of Human Rights, is one of the most important documents

---

of "its inability to provide adequate support for sections of its membership who were on strike." *Id.* This was especially unfortunate at a time when the very principle of trade unionism was on the defensive. A Web of English History, *The Grand National Consolidated Trade Union* (taken from H. Pelling, *A History of Trade Unionism*), *at* http://dspace.dial.pipex.com/town/terrace/adw03/peel/trade-us/gnctu.htm (last modified Dec. 5, 2004).

236. The Industrial Revolution, *supra* note 228.

237. *See, e.g.*, Council of Europe, *Council of Europe Portal, at* http://www.coe.int/DefaultEN.asp (last updated May 27, 2005).

238. The Convention is respected in the European Community through Maastricht Treaty of 1992 and stated as the general principles of E.U. law.

underlying the right to privacy.[239] Individuals can file a complaint to this Court provided all national remedies have been exhausted. During the last few decades European policymaker have discussed what comprises the private sphere. It is important to understand how the European Court of Human Rights and the Convention for the Protection of Human Rights and Fundamental Freedoms work in order to understand the European law of electronic monitoring. Most privacy-based legislation in Europe, including statutes governing personal data, privacy, and protection of e-mails, has its genesis in the Council of Europe's Convention.

a. The Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms of 1950

In Modern Europe, the devastating impact of two World Wars left the continent fractured, displacing individual rights. After the Second World War, the countries of Europe banded together to develop community-wide legislation to protect individual human rights. The Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 (ECHR) reflects a Europe-wide movement to guarantee individual rights.[240] The ECHR is a legal norm incorporated by reference into the national legislation of each member state. Since the vast majority of European countries are civil code jurisdictions, the ECHR is self-executing.[241] The European Court of Human Rights is a special court, situated in Strasbourg, and is the principal enforcement agency of the Convention. The Court receives its mandate under the ECHR as amended

---

239. Registrar of the European Court of Human Rights, *The European Court Of Human Rights: Historical Background, Organisation and Procedure* (Sept. 2003), *at* http://www.echr.coe.int/Eng/EDocs/HistoricalBackground.htm.

240. Article 8 of the ECHR is about the Right to Respect for Private and Family life. Article 8 says:

> (1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

ECHR, *supra* note 209.

241. In a civil code jurisdiction, the convention has a self-executing effect as soon as it is duly signed and ratified. In England, which is a common law country, a convention does not come into effect until it has been enacted into domestic law by an Act of the Parliament. The Human Rights Act in England came as late as 1998 and did not come into force until 2000, despite the fact that England was the first member state to sign the Convention. Eurolegal Services, *UK Human Rights*, *at* http://www.eurolegal.org/british/ukhumanrights.htm (last updated Mar. 14, 2005).

by Protocol 11,[242] and is available to any contracting state or individual when all domestic remedies are exhausted.[243] All final judgments of the European Court of Human Rights are binding on the respondent states, and the Committee of Ministers of the Council of Europe supervises the execution of the judgments.[244]

Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms expressly states: "Everyone has the right to respect for his private and family life, his home, and his correspondence."[245] The European Court of Human Rights has extended the definition of "private life and correspondence" as articulated in Article 8 to include all business relations as well as e-mail and other electronic communications.[246] Article 8 of the ECHR articulates a basic fundamental right to privacy embodied in the constitutions of European countries,[247] and grants all Europeans the fundamental right to have their privacy respected.[248] Since the enactment of the ECHR, there have been a few cases interpreting what the right to private life means in specific contexts.

In *Niemietz v. Germany*,[249] the European Court of Human Rights expanded the meaning of "private life" from the "inner circle" of an individual's life to also include the right to establish and develop relationships with other human beings.[250] The *Niemietz* decision is a useful precedent for extending the ECHR to encompass workplace privacy. The Court also raised concerns in a situation where governments were to make a clear distinction between private life and professional life. They contended that such a distinction would likely lead to unequal treatment.[251] The *Niemietz* court's ruling that Article 8 would only be triggered if professional life and private life were so intermingled that there is no

242. Protocol 11 (ETS No. 55) entered into force November 1, 1998.

243. The procedure is adversarial and public. *The European Court of Human Rights: Historical Background, Organization and Procedure*, *supra* note 239.

244. The Committee of Ministers of the Council of Europe consists of the Ministers of Foreign Affairs of the member states or their representative. *Id.*

245. European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, art. 8, 213 U.N.T.S. 221.

246. Niemietz v. Germany, 251 Eur. Ct. H.R. 23 (1992); Halford v. United Kingdom, 39 Eur. Ct. H.R. 1004 (1997).

247. Frank Hendrickx, *Legal Regulation of Disclosure of Information About Employees or Prospective Employees to Employers or Prospective Employers in Belgium*, 21 COMP. LAB. L. & POL'Y J. 651, 653 (2000) (noting that Article 8 is a "basic source of law to be mentioned. . . the constitutional right to privacy," which is also protected by Article 22 of the Belgian Constitution).

248. However, it is important to point out that Article 8 does not give an absolute right to privacy, but the right to have privacy respected. *See* ECHR, *supra* note 209.

249. *Niemietz*, 251 Eur. Ct. H.R. at 23 (discussing a search of a lawyer's office, based on a broad search warrant).

250. *Id.* at 33.

251. *Id.*

means to distinguish between them is promising, though it refused to make such a distinction in that case.[252] The *Niemietz* court states that the meaning of the word "correspondence" is not limited to private correspondence, and concludes that Article 8 protects correspondence regardless of whether it is private or professional.[253]

In *Halford v. United Kingdom Government*,[254] the European Court of Human Rights considered the issue of whether Article 8 of ECHR applied to the interception of personal phone calls at work. In *Halford* the applicant had applied several times for a promotion as an Assistant Chief Constable in the police force where she was working, but was denied the position every time.[255] Ms. Halford commenced a proceeding against the Chief Constable and the Home Secretary for discrimination for failing to promote her on grounds of sex.[256] Certain of her co-workers in the police force launched a campaign against her, which led to leaks to the press and secret interception of her phone calls, both at home and at her office.[257] The information obtained by tapping her office and her home phones was used against her in the discrimination proceeding and led to the decision to bring a disciplinary proceeding against her.[258]

The *Halford* court held that the surreptitious interception of private calls made by Ms. Halford from her office was in fact an unjustifiable interference with her right to privacy and correspondence.[259] The reasoning employed by the European Court of Human Rights applies equally well to any monitoring or recording of private correspondence contained in e-mail, faxes, wireless communications, and all technological means of correspondence.[260] In *Halford*, the government attempted to formulate a

---

252. *Id.*

253. *Id.* at 34. *See* Huvig v. France, 176 Eur. Ct. H.R. 36, 41, 52 (1990) (discussing where the search was directed solely against business activities and documents, including wiretapping of applicant's telephone, but the court did not even advert the possibility that Article 8 might be inapplicable just because the correspondence was of professional character and held that there had been a violation of Article 8).

254. Halford v. United Kingdom, 39 Eur. Ct. H.R. 1004 (1997).

255. *Id.* at 1009. In order to get the position she needed an approval from the Home Office, which was withheld by the Chief Constable.

256. *Id.* at 1009.

257. *Id.* at 1009–10. Halford had two phones in her office, one of which was for private use, but both were part of the internal police telephone network that is classified as a "public" telecommunication system." Neither restriction nor guidance of how to use either phone was give to Halford; however, Halford received memoranda allowing her to use the "private" phone for the purposes of her sex-discrimination case. *Id.* at 1010, 1012.

258. *Id.* at 1010–11.

259. The court recognizes that the applicant had a reasonable expectation of privacy, especially since she had no prior warning about the interception and was granted to use the phones for delicate private matters. *Id.* at 1015–16.

260. *Internet and E-Mail Policies*, ACAS ADVICE LEAFLET (Acas, London, U.K.), Mar. 2004, *available at* http://www.acas.org.uk/publications/AL06.html (last visited May 4,

property-based argument similar to American law, contending that an employer should be able to monitor telephones provided by the employer without providing the employee notice.[261] The *Halford* court refused to make any distinction between professional and private correspondence in order to protect one group of correspondence more or less than the other.[262] This critically important precedent is emblematic of the court's unwillingness to accept the bifurcated distinction between the private and public spheres so well established under American law. The *Halford* case is also important because it demonstrates that the court is unwilling to accord employers the right to monitor merely because they have a property interest in information technologies.[263] Private correspondence does not lose its status as private simply because devices at work, in the office, are used. Private communications remains private regardless of what technologies are employed, which is a fundamentally different approach to the American property-based and contract-based regime for electronic surveillance.[264]

The *Halford* court also noted that when it comes to secret "surveillance or interception of communications by public authorities, there is an additional concern because of the danger that power will be abused."[265] The court expressed its concern that secret surveillance is marked by a lack of public scrutiny and that domestic national law must provide remedies as well as protection to the individual against arbitrary interference with Article 8 rights.[266] This clearly demonstrates that the European Court of Human Rights is predisposed to policing cases in which employers misuse their power by intercepting electronic communications. Thus, European employees have greater protection than their American counterparts.

3. Initiative by the European Union

European labor law is largely governed by national legislation, which means that there will be variations in protections granted to workers. The Treaty of The European Union recognizes the European Convention for the Protection of Human Rights and Fundamental Freedoms and requires each member state to respect the fundamental right of privacy.[267] In addition,

---

2005).

261. *Halford*, 39 Eur. Ct. H.R. at 1016.

262. *Id.* (following *Huvig* and *Niemietz*).

263. *Id.; see, e.g.*, McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 Tex. App. LEXIS 4103 (Tex. App. 1999).

264. *See* Part I *infra*.

265. *Halford*, 39 Eur. Ct. H.R., at 1017.

266. *Id.*

267. Lasprogata et al., *supra* note 15, at ¶ 8.

the European Community (EC) has enacted basic guidelines that all member states must follow and that raise the bar for workers rights.[268] The general policy of the EC has been to promote, protect and enable the development of the Internet in a single market, since the promotion of technology is so important for the economy and society. In the March 2000 Lisbon Meeting of The European Council, the E.U. proposed a new strategic goal for the next decade "to become the most competitive and dynamic knowledge-based economy in the world, capable of sustainable economic growth with more and better jobs and greater social cohesion."[269]

Europe's dual enforcement system has its roots in the harmonizing principles of the Rome Treaty.[270] The E.U. formed new legal institutions to carry out its objective of shrinking national borders and ensuring greater competition. Each head of state of the forty-six member states belongs to the Council of the European Union, which is a major policy-making institution responsible for whatever matters are on the particular agenda: foreign affairs, farming, industry, transport, or emergent issues.[271] The European Parliament is the elected body representing the 452 million E.U. citizens and consists of 732 directly elected representatives of member

---

268. *See* Community Charter of Fundamental Social Rights for Workers (1989) (giving member states a minimum provision for employment and working conditions). *Activities of the European Union, Summaries of Legislation, Anti-Discrimination, Fundamental Social Rights and Civil Society, at* http://www.europa.eu.int/scadplus/leg/en/cha/c10107.htm (last visited May 4, 2005).

269. Also referred to as the Lisbon Switch Strategy. Europa, *Employment and Social Affairs, European Employment Strategy, at* http://europa.eu.int/comm/employment_social/employment_strategy/index_en.htm (last updated Sept. 28, 2004). In 2003, surveys showed that in Sweden and Finland over ninety percent of all enterprises of all sizes were connected to the Internet, on average this percentage was about seventy-three percent in the E.U. *New Technology and Respect for Privacy at the Workplace, supra* note 207.

270. Article 2 of the Treaty of Rome states the following principle:

> The Community shall have as its task, by establishing a common market and an economic and monetary union and by implementing the common policies or activities referred to in Articles 3 and 3a, to promote throughout the Community a harmonious and balanced development of economic activities, sustainable and non inflationary growth respecting the environment, a high degree of convergence of economic performance, a high level of employment and of social protection, the raising of the standard of living and quality of life, and economic and social cohesion and solidarity among Member States.

TREATY ESTABLISHING THE EUROPEAN COMMUNITY, Nov. 10, 1997, O.J. (C 340) 3 (1997), art. 2 [hereinafter EC TREATY], *available at* http://europa.eu.int/abc/obj/treaties/en/entr6b.htm#Article_2 (last visited May 22, 2005).

271. The European Council is a key decision-making institution, which is responsible for foreign affairs, farming, industry, transport or other emergent issues. Europa, *Activities of the European Union: Summaries of Legislation, Anti-Discrimination, Fundamental Social Rights and Civil Society, at* http://www.europa.eu.int/scadplus/leg/en/cha/c10107.htm (last visited May 28, 2005).

states.[272] The European Court of Justice (ECJ) in Luxembourg ensures member states' compliance with the legislation of the European Union.[273] The European Commission is the chief institution to develop legal frameworks for the Internet to advance free competition in the single market. It is also the principal formulator of privacy law, because it is a body with powers of initiative, implementation, management, and control.[274] The Commission approved the E.U.'s key related directives: the E-Commerce Directive, E-Signatures Directive, Distance Selling Directive, Data Protection Directive, Database Protection Directive, and the Copyright Directive.[275]

The still-evolving European Union will have a greater influence on the path of Internet privacy now that accession is completed.[276] In order to

---

272. *Id.*

273. For more information about the European Court of Justice, *see* CVRIA, *The Court of Justice of the European Communities*, *at* http://www.curia.eu.int/ (last visited May 28, 2005).

274. *European Parliament*, *supra* note 271.

275. Directives must be implemented by each Member State. However, there is no consistent pattern in implementing E.U. Directives. For example, only four Member States enacted legislation implementing the Data Protection Directive within the October 1998 deadline agreed to "when they adopted the Directive in the Council.

> The Commission decided in December 1999 to take France, Germany, Ireland, Luxembourg and the Netherlands to the European Court of Justice. Germany and the Netherlands, along with Belgium, then implemented the Directive in 2001 and Luxembourg, after the Court found against it, implemented the Directive in 2002. More than seven years after the adoption of the Directive and more than four years after the deadline for its implementation (Oct. 1998), France has still not yet passed the legislation necessary to bring its old data protection law of 1978 fully into line with the Directive.

Press Release, Commission of the European Communities, Data Protection: Commission Report Shows That EU Law Is Achieving its Main Aims (May 16, 2003), *available at* LEXIS, European Union database.

276. The European Union has recently been enlarged with ten new member states from eastern and southern European countries, including Czech Republic, Estonia, Cyprus, Latvia, Lithuania, Hungary, Malta, Poland, Slovenia, and Slovakia. Additionally, the E.U. is currently preparing the accession of four other countries: Bulgaria, Romania, Croatia, and Turkey. *European Parliament*, *supra* note 271. In Eastern Europe countries such as Romania and Bulgaria, there is a presently low computer and Internet usage rate. A survey found "Internet availability and access is very high, with an average of 90% of the respondents reporting that they have Internet access. The lowest penetration was in Romania, in which roughly a quarter, 50 of 209 respondents, reported not having Internet access. The PC usage was also lower in Romania. Of the companies that have Internet access, a varying number of employees make regular use of the Internet in their work routine. On average Polish SMEs have a relatively high level of usage, while fewer employees regularly use the Internet in Romania, Cyprus, and Bulgaria." JNN & Associates, *eBusiness in Southeastern Europe: Facts and Figures*, *at* http://www.jnn-marketing.com/index.php?p=an1_2003&mt=free (last visited May 28, 2005).

make the relationship between the Convention on Human Rights of the European Council and the protection of privacy in the European Union clearer, we will first explain their relationship and compare the specific articles comparable to Article 8 ECHR. Next, we will describe the main directives on privacy in the European Union and show how those directives can be applied to an employment context, where the unions struggle for workers' rights in the technological revolution, instead of in the Industrial Revolution.[277]

a. E.U. Protections for Private Life and Personal Data

In 2000, in Nice, the European Union proclaimed the Charter of Fundamental Rights of the European Union (the Charter) in order to catalogue the fundamental rights of Europe's citizens, which are somewhat based on the case law of the European Court of Human Rights in Strasbourg and the ECJ in Luxembourg.[278] The Charter was an effort to bring together all the rights that were spread out in several different legislative instruments, such as the Convention from the European Council, documents from the United Nations, and national laws.[279] The Charter protects the traditional rights (e.g., right to life, freedom of expression) as well as more modern rights such as data security and security of communication regardless of means used.[280]

Articles 7 and 8 in the Charter of Fundamental Rights of the European Union protect private and family life and personal data.[281] In drafting Article 7, the authors of the Charter took the technological evolution into account by replacing the term "correspondence," used in Article 8 of the ECHR, with "communications." This change in wording guarantees protection for communications regardless of the means of communication

277. "The OECD Guidelines and the 1981 Council of Europe Convention each incorporates rules that require personal data protection from collection through dissemination, and guarantee the right of individuals to access information collected about them and make changes where necessary to correct inaccuracies." Lasprogata et al., *supra* note 15, at ¶13.

278. Charter of Fundamental Rights of the European Union, Dec. 18, 2000, 2000 O.J. (C 364) 1 [hereinafer Charter], *available at* http://www.europarl.eu.int/comparl/libe/elsj/charter/default_en.htm.

279. The Charter helps to develop the concept of citizenship of the European Union and to create an area of freedom, security and justice, as laid down in the preamble. The Charter also enhances the legal security of the protection of fundamental rights. *Id.*

280. Today every new legislative instrument produced by the E.U. must contain this statement: "this act respects the fundamental rights and observes the principles recognized in particular by the Charter of Fundamental Rights of the European Union as general principles of Community." However, the Charter will not be fully legally binding until the proposed Constitution of the European Union is adopted. *Id.*

281. *Id.* at art. 7.

used.[282] This means that even in the formulation of the right to correspondence, the E.U. did not distinguish between the types of means used for the communication, which the U.S. clearly has done through case law by giving e-mail less protection than phone calls.[283]

The Charter also makes the right of protection of personal data a separate fundamental right in Article 8, distinct from the general privacy accorded to family life and communications.[284] The guaranteed protection of personal data covers the processing of this data as soon as it enters the boundaries of the Union or comes within the scope of E.U. institutions and bodies, irrespective of the medium used.[285] Furthermore, the right to protection of personal data must be balanced with freedoms of expression and information, which means that even if the information is personal data, the public interest value of that information might be so strong that it prevails, and the information becomes public.[286] Regardless of the outcome, the opposing interests must be weighed in each individual case, and in Europe, the bar to get the information to the public is much higher than in the U.S. The U.S. tends to be more protective of media rights, such as the right to free speech which is protected in the Constitution, than the right of privacy.

b. Directives Protecting Privacy and Personal Data

Each member state of the E.U. follows a dual system of regulation composed of national legislation and E.U. regulations.[287] When it comes to

---

282. Article 7 states that "everyone has the right to respect for his or her private and family life, home and communications," and is equivalent to Article 8 ECHR. *Id.*

283. American courts have distinguished between private and professional mail, but not between personal and professional e-mails. *See Ex parte* Jackson, 96 U.S. 727 (1878); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002); Vernars v. Young, 539 F.2d 966 (3d Cir. 1976). E.U. policy on telecommunications and electronic communications services is regulated by Directive 2002/58/EC of July 12, 2002 (replacing the Directive 97/66/EC of December 15, 1997). European Parliament and Council Directive on Privacy and Electronic Communications, 2002/58/EC, art. 4, 2002 O.J. (L. 201) 37, *available at* http://europe.eu.int/eurlex/pri/en/oj/dat/2002/1_201/1_20120020731en00370047.pdf (last visited May 22, 2005). The Telecommunications Directive adopts the concept of technological neutrality that parallels Article 7 of the Charter, seeking to avoid measures favoring or disfavoring any specific communication means. *Id.* The goal of the Directive is to ensure an equivalent level of user protection, irrespective of the service used. *Id.*

284. Charter, art. 8 (providing rules governing protection of personal data), *available at* http://www.europarl.eu.int/comparl/libe/elsj/charter/art08/default_en.htm (last visited May 22, 2005).

285. *Id.*

286. This right includes "the freedom to receive and impart information and ideas without interference by public authority and regardless of frontiers." ECHR, art. 10; *see also* Charter, art. 11 (elaborating on Article 10 of the ECHR).

287. The 1957 Treaty of Rome created new legal institutions designed to harmonize the

Internet regulation, the E.U. follows a command and control model that is more rule-oriented than the market-driven approach of the United States. European competition law, for example, favors bright-line rules for determining anti-competitive behavior, in contrast to the broad standards of the Sherman Antitrust Act.[288] When an E.U. directive is adopted, the member states normally have a certain transition time to implement the rules into their national legislation.[289]

In October 1995, the EC adopted a directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data between member states.[290] This Directive applies to all data, processed both by automatic means (e.g., computers) and by traditional non-automated filing (e.g., paper files). It ensures the rights and freedoms of natural persons with respect to processing personal data and describes when such processing is lawful.[291]

All Europeans have the right to privacy in the collection of personally identifiable data and the right to have their personal information protected by adequate security.[292] The Data Protection Directive gives data subjects control over the collection, transmission, or use of personal information.[293] The data subject also has the right to be notified of all uses and disclosures about data collection and processing.[294] All companies, for example, are required to obtain explicit consent as to the collection of data on race/ethnicity, political opinions, union membership, physical or mental

---

law. The purpose of uniform laws throughout Europe is to facilitate commerce and reduce transaction costs in cross-border transactions. Directives are formulated by the European Commission, finalized by the European Parliament and adopted by the European Council. TREATY OF ROME, *supra* note 270.

288. A good example of greater emphasis on rules is Article 82 of the EC treaty. EC TREATY art. 2. Article 82 attempts to prevent price-fixing and other unilateral activities. *Id.* In order to be liable for price-fixing, the anticompetitive entity must have a dominant position defined as at least fifty percent control of the market. *See* Jessica Natale, *Practice Pointer: Complying with EU Competition Law*, *in* E-BUSINESS LEGAL HANDBOOK, 8–117 (Michael Rustad & Cyrus Daftary eds., 2003).

289. This transition time is normally two to five years depending on how complicated and extensive the directive is. After the transition time is up, the directive will be enforced to the benefit of the citizens regardless if the member state has implemented the directive or not. If the directive has direct effect that will say if the directive is so clear and precise.

290. *See* Council Directive 95/46/EC, 1995 O.J. (L 281) 31 (governing the protection of individuals with regard to the processing of personal data).

291. *Id.*

292. *Id.* at arts. 1, 17.

293. *Id.* at arts. 6, 10, 11, 12. The European Commission has published a guide named "Data protection in the European Union," which provides citizens and businesses with information about their rights regarding the collection and use of personal information. EUROPEAN COMMISSION, DATA PROTECTION IN THE EUROPEAN UNION, *available at* http://www.europe.eu.int/comm/justice_home/fsj/privacy/docs/guide/guideukingdom_en.pdf (last visited May 22, 2005).

294. Council Directive, *supra* note 290, at arts. 12, 14.

health, sex life, and criminal records.[295] Data subjects have the right to obtain copies of information collected as well as the right to correct or delete personal data.[296]

The general principles in the Data Protection Directive were expanded by a new Directive on Privacy and Electronic communication in 2002, which targets specific privacy issues relating to electronic communications.[297] The directive specifically states that the confidentiality of communications prohibits the practice of interception or surveillance of private communications between others over networks.[298] This is an extension of the protection already recognized for private phone calls to also include e-mails, SMS and MMS messages.[299] Gaining access to or storing information from a user's terminal (e.g., PC, mobile phone or other similar devices) 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.[300] The Directive on Privacy and Electronic communication primarily focuses on public communication networks and does not necessarily include internal work e-mails.

This means that though public employees are directly protected against surveillance under this directive, it does not necessarily follow that private employees' communications are protected on internal networks. However, when private employees access a public network, these regulations automatically protect them. Employers are left with a limited area of employee communication that they can monitor according to these directives. This shows that the directives do not adequately protect employees in all aspects against monitoring and surveillance by their employers. This problem has been raised by the European Commission, which is trying to develop a new directive specifically targeting the protection of workers' personal data, with the collaboration of trade unions and employers' organizations, in order to find a balance.

---

295. *Id.* at arts. 7(a), 8(2).

296. *Id.* at art. 12.

297. The EC has also created some guidelines when it comes to privacy on the Internet in their Recommendation 2/2001 "on certain minimum requirements for collecting personal data on-line in the European Union." *See* European Union, Data Protection *at* http://europa.eu.int/information_society/topics/ecomm/all_about/todays_framework/privacy_protection/index_en.htm (last visited May 4, 2005).

298. Council Directive on Privacy and Electronic Communication, *supra* note 283, at art. 5(1) (prohibiting listening, tapping, storage and other kind of interception or surveillance of communication without consent).

299. European Commission, *Privacy Protection*, *at* http://europa.eu.int/information_society/topics/ecomm/all_about/todays_framework/privacy_protection/index_en.htm (last updated Dec. 5, 2004).

300. Council Directive on Privacy and Electronic Communications, *supra* note 283, at art. 5(2).

c. The E.U. Directives in an Employment Context

The European Commission launched a consultation in 2001 asking its social partners about the protection of workers' personal data and whether they believed that the protections granted by the two personal data directives, Data Protection Directive 95/46/EC and Directive on the Protection of Privacy 97/66/EC, were enough.[301] The responses to the consultation showed that all of the social partners agreed upon the importance of the question of the privacy of personal data processing in the employment context, particularly considering the socioeconomic and technological developments of the last years.[302] However, there were many disagreements between employers' associations and trade unions about how the E.U. should continue its actions.[303]

The employers' organizations thought that the existing directives were appropriate and capable of ensuring that workers' personal data is protected.[304] They rather emphasized the importance of flexibility and national diversity, as well as the risk of over-regulation and the undue burden on employers.[305] These organizations favored awareness, best practice rules and non-binding national instruments.[306] Trade unions, however, argued that the two directives in place were too general and that there is a need for more specific rules about privacy regarding electronic communications at work.[307] Further, they did not think that the national legislation in place was totally satisfactory.[308] Even with the broad European regulation in this area, trade unions believed that employers have an unfair privilege in monitoring their employees.

Based on the outcome of the first consultation, the European Commission launched a second consultation with the aim of visualizing a proposal for a new directive for a framework of employment-specific rules on data protection in the workplace.[309] One of the reasons for the

---

301. Catherine Delbar et al., *New Technology and Respect for Privacy at the Workplace*, EUR. INDUS. REL. OBSERVATORY ONLINE, Dec. 8, 2003, *at* http://www.eiro.eurofound.eu.int/2003/07/study/TN03071018.html.

302. European Commission, *Second Stage Consultation of Social Partners on the Protection of Workers' Personal Data*, 2 *at* http://europa.eu.int/comm/employment_social/labour_law/docs/secondstageconsultationdataprot_en.pdf (last visited May 22, 2005).

303. *Id.* at 3.

304. *Id.*

305. *Id.*

306. *Id.*

307. *Id.* at 3, 7.

308. *Id.*

309. Andrea Boughton, *Commission issues second stage consultation on data protection*, EUR. INDUS. REL. OBSERVATORY ONLINE, Nov. 20, 2002, *at* http://www.eiro.eurofound.eu.int/2002/11/feature/eu0211206f.html. The Commission is planning a draft of a new Directive in 2004 or 2005 according to its mid-term review

framework is to be able to promote and ensure that European workers become more mobile and still have a boundary between work and private life. Some other reasons are globalization, the trend of outsourcing human resources, and insecurity after September 11, 2001.[310] This new directive would deal with issues such as consent, medical data, genetic testing, monitoring and surveillance, seeking especially to clarify the legal environment for monitoring and surveillance, as well as to ensure compliance with fundamental human rights.[311] Clarification of monitoring and surveillance laws is also important because advanced information technologies are more intrusive on private life than traditional telephone-tapping and video surveillance.[312] E-mail and Internet monitoring threatens to erode workers' privacy.[313] The proposal advocates greater consultation by anyone handling personal information. The proposed regime imposes restrictive monitoring rules in the employment context.[314] Under the proposal, in order to monitor a specific worker, the employer must have reasonable suspicion of criminal activities or serious wrongdoing or misconduct, and there must be no less intrusive means available.[315] The opening of private e-mails and files would be totally prohibited, irrespective of whether personal use of these work tools was authorized, all private electronic communications are protected as "private correspondence" in light of the ECHR and the Charter of Fundamental Rights of the European Union.[316] This approach is fundamentally equivalent to the way France already deals with privacy of correspondence at work.

d. The Position of the European Court of Justice

The ECJ has pointed out the importance of companies having written and signed e-mail policies on hand in order to enforce them and to monitor employees' e-mail communications. This is contrary to the willingness of U.S. courts to validate secret surveillance of e-mail even if the company assured its employees that all e-mail would remain confidential and

(European Commission, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Mid-term Review of the Social Policy Agenda, COM (2003) 312, at 16). As to date, the Commission has not yet produced such a directive.

310. *Id.* at 8.
311. *Id.* at 9.
312. Delbar et al., *supra* note 301, at 6.
313. *Id.*
314. *Id.*
315. *Id.*
316. *Id.*

privileged.[317] However, the ECJ has not yet decided a case about employers' general right to monitor employees' Internet and e-mail use. However, the court validated an employer's Internet policy in *X v. European Central Bank*.[318] After an internal investigation, the bank's investigators found that X, an employee of European Central Bank (ECB), was downloading and transmitting pornography and political documents to third parties using his work computer.[319] X transmitted pornographic materials to an ECB coworker who objected to these materials. The coworker felt that she was being sexually harassed with these inappropriate communications and complained to X on several occasions that he had no right to transmit these materials.[320] X was suspended by the ECB after an investigation of his inappropriate use of e-mail and the Internet.[321] The applicant in *ECB* did not challenge the financial institution on grounds of invasion of privacy, but rather on the contractual validity of its Internet policy.[322] The contractual ECB policy expressly provided that the bank's Internet technologies were for business use only, and by downloading pornographic files and harassing co-workers by sending them the files, X clearly misused the Internet at work.[323] The *ECB* court upheld the suspension, concluding that the bank had the right to set up internal disciplinary rules for breaches of employment agreements.[324] Because the employee agreed not to abuse the computer system as a condition of employment, the bank's disciplinary action was within the contract of employment.[325] *ECB* demonstrates that a company has the right to draw up internal employment rules about misuses of Electronic communication that constitute immoral, criminal acts.

317. *See, e.g.*, Smyth v. Pilsbury Co., 914 F. Supp. 97, 98, 101 (E.D. Pa. 1996) (finding no reasonable expectation of privacy in the employee's e-mail communications even though the employer repeatedly assured that all the e-mail communications would remain confidential and privileged).

318. Case T-333/99, X v. European Central Bank, 2001 E.C.R. II-3021, IA-00199, II-00921 (2001), *available at* http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=61999A0333&model=guichett (last visited May 22, 2005).

319. *Id.* at 5, para. 8.

320. *Id.* at 5, para. 13.

321. *Id.* at 5, para. 8.

322. *Id.* at 7, para. 27.

323. *Id.* at 4, para. 5.

324. The court concluded that ECB had the capacity to set up disciplinary contractual rules according to its Conditions of Employment, which X had signed and agreed to, and dismissed all of plaintiff's claims.

325. *Id.* at 15, paras. 87–88.

C. United Kingdom Law & Policy

The EC has promulgated privacy protection in several directives encompassing "constitutional law, employment law, data protection and telecommunications legislation."[326] Yet, the European member states vary in the extent of their privacy protection. Sweden, for example, has yet to enact a comprehensive privacy statute applicable to electronic technology.[327] In Sweden, there are a large number of teleworkers but courts have provided no real guidance on the electronic monitoring of e-mail or Internet usage.[328]

This section focuses on legal developments in the United Kingdom (U.K.) because it is a common law country and the cradle of Anglo-American tradition. In the next sub-section we compare the U.K. approach to the French civil law tradition. We briefly discuss the emerging problem of telecommuting employees, recognizing the growing trend of "traveling" or telecommuting employees who are connected and available to their employers 24/7, but not necessarily in a fixed location.[329] Our overwhelming finding is that the laws of e-mail and Internet monitoring for the U.K. and France diverge markedly from the path of U.S. law.

The U.K. is the only European country that follows the common law system and has a similar legal structure to America. Even though there is a shared common law heritage, there is little harmony between the law of electronic monitoring in the U.S. and in the U.K. In some respects, this divergence can be explained by the U.K.'s membership in the E.U., which requires it to follow the fundamental rights approach honed in civil law jurisdictions. Under the European Community Treaty, the U.K. must implement enabling legislation to carry out the fundamental rights as set

---

326. *Submission to the Victorian Law Reform Commission on its Issues Paper into Workplace Privacy*, VLCR INQUIRY INTO WORKPLACE PRIVACY (Office of the Victorian Privacy Comm'r, Melbourne, Australia), Apr. 11, 2003, at 5, *available at* http://www.privacy.vic.gov.au/dir100/priweb.nsf/0/5d37ecb57a98bda7ca256c4d0019e8ad?OpenDocument&ExpandSection=5.

327. *See, e.g.*, Reinhold Fahlbeck, *A Comparative Study of the Impact of Electronic Technology on Workplace Disputes: Electronic Technology and Work: A Swedish Perspective*, 24 COMP. LAB. L. & POL'Y J. 257 (2002).

328. *See id.* (stating that privacy-related provisions can be found in many statutes, but are not always well synchronized). The 1998 Personal Data Protection Act is the single most important piece of legislation. Case law on employer monitoring is nonexistent. Fahlbeck contends that Article 6 of Chapter 2 of the Personal Data Protection Act may be extended to electronic surveillance. This Article states: "[A]ll citizens shall be protected in their relation with the public realm against . . . examination of mail or other confidential correspondence and against secret tapping or recording of telephone calls or other confidential communications." Fahlbeck futher argues that "[a]lthough this rule appears to be comprehensive in its prohibitions, Article 12 of the same chapter permits limitations, albeit only to achieve a purpose acceptable in a democratic society." *Id.* at 265.

329. *Id.* at 264.

forth in the ECHR and the legislation of the E.U. These two bodies of law are vital to the development of the U.K.'s law of e-mail surveillance.

In the U.K., as in the U.S., employers routinely implement software-based employee monitoring solutions.[330] A survey of more than two hundred British firms found that these companies terminated sixty-one employees for abuse of e-mail and the Internet at work in 2002.[331] Seventy percent of all the U.K.'s Internet pornographic transmissions took place during the nine-to-five workday, which is a finding that supports the employer's need to monitor electronic commissions.[332] Further, an estimated thirty to forty percent of U.K. workplace computer usage is not related to work.[333] The estimated cost to employers for unauthorized workplace access to Channel 4's Big Brother series was •300,000 per day.[334] An estimated two-thirds of personal online purchases of goods and services in the U.K. are made on office computers during the workday.[335] All of these surveys demonstrate that the misuse of electronic communications is a widespread problem.

1. Legislation on Internet Monitoring

The U.K. has adopted a predominately regulatory approach to Internet and e-mail monitoring in the workplace as opposed to relying heavily upon market-based incentives, as in the U.S. The British Prime Minister promised that the government would ensure that everyone in the U.K. who wants access to the Internet should have it by 2005.[336] The principal reason for this initiative was the government's desire to promote business and economic growth. However, the government tacitly accepted the right of businesses to monitor their employees.[337] As in the U.S., the doctrine of vicarious or imputed liability makes U.K. employers generally liable for acts committed by employees within the scope of their employment duties.

---

330. *See* Ingenuity (UK) Ltd., *Welcome to Ingenuity (UK) Ltd*, *at* http://www.ingenuity.co.uk/ (last visited May 28, 2005) (describing Ingenuity (UK) Ltd.'s software that monitors employees' Internet usage).

331. Andrew Bibby, *Electronic Monitoring in the Workplace*, FREELANCER.DK (2002), *at* http://www.freelancer.dk/default.asp?pageToLoad=visNyhed%2Easp%3FartikelID%3D248.

332. *See* Eugenie Houston, *E-mail Privacy at Work*, MONSTER HUMAN RESOURCES (2002), *at* http://hr.monster.ie/articles/email_privacy/print/ (citing a study performed by the British research firm Websense).

333. *Id.*

334. *Id.*

335. *Id.*

336. CABINET OFFICE, ELECTRONIC COMMUNICATIONS AT WORK: WHAT YOU NEED TO KNOW (2d ed. 2001), *at* www.e-envoy.gov.uk/assetRoot/04/00/54/55/04005455.pdf.

337. Courts in the U.K. have not yet handed down decisions shaping the law of e-mail monitoring in the workplace.

Excessive private use of communications facilities at work can corrode the efficiency of the company, disturb security, and expose the company to lawsuits.[338] But, at the same time, the U.K. does not allow surreptitious monitoring by the employer as in America. The U.K. balances the right of employers to monitor against workers' privacy rights, by prohibiting secret monitoring.

There are five main statutes that regulate Internet monitoring in the U.K., and to date there are few cases. The Data Protection Act of 1998[339] was the implementation of the European Data Protection Directive concerning the right of freedom for individuals regarding the processing of personal data. The Human Rights Act of 1998 and OFTEL Guidance on Recording on Private Telephone Conversations of 1999, were both enacted in response to the *Halford* case decided by the ECHR in 1997, concerning the respect of private communication at work according to Article 8 HCHR.

Finally, the Regulatory of Investigatory Powers Act of 2000 closely tracks the Lawful Business Practice Regulations of 2000, which provides the ground rules for when employers may intercept and monitor e-mails and Internet access at work. If an employer breaches the Data Protection Act, for example, he is subject to civil and criminal liability and may be fined up to £5,000.[340] In stark contrast to the pro-employer regime of electronic surveillance in America, the U.K.'s regulatory regime arms the victims of abusive monitoring with meaningful remedies.

a. Data Protection and Privacy

British employers' electronic surveillance of their employees' e-mail and Internet usage must comply with the U.K.'s implementation of the European Union Directive on Data Protection. The U.K. Data Protection Act (DPA), enacted in 1998, provides another remedy against abusive 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 according to special "Data Protection Principles."[341] The DPA carves out one exception to the notice requirement: It allows surveillance without notification when electronic

338. CABINET OFFICE, *supra* note 336.

339. Council Directive 95/46/EC, 1995 O.J. (L 281) 31.

340. ROBERT MUCKLE SOLICITORS & WATERFORD TECHNOLOGIES, E-MAIL MONITORING IN THE WORKPLACE: A SIMPLE GUIDE TO EMPLOYERS 1 (July 2003).

341. These principles can be summarized into: fairly and lawfully processed; processed for limited purposes; adequate, relevant and not excessive information; accurate; not kept longer than necessary; processed in accordance with the data subject's rights, secure and not transferred to countries without adequate protection. NICK HIGHAM & SARA ELGSTRAND, DENTON, WILDE AND SAPTE, DATA PROTECTION OVERVIEW § 2 (2001).

monitoring is done for the purpose of preventing a specific crime.[342] The DPA requires that all monitoring be lawful and fair to employees, to protect personally identifiable data.[343] Further, a monitoring program must be reasonably related to achieving a legitimate business purpose while respecting the privacy of individuals.[344] It would not, for example, be a violation of the DPA for a system's administrator to access files in order to detect and remove a computer virus from the system, since this act would not involve reading the content of incoming e-mails.

The DPA also takes into account the requirements of the Human Rights Act of 1998 (HRA).[345] The HRA has yet to explicitly define the meaning of privacy in judicial decisions, but it is clear that "private correspondence is expressly protected, alongside telephone and e-mail communications."[346] When it comes to employment claims under the HRA, the statute distinguishes between public and private sector employers. If the employer falls into the public category, the employee has a direct cause of action under the ECHR.[347]

As in the other countries of the EC, workers in the U.K. are also protected by Article 8 of the ECHR, which generally respects family life, the home, and correspondence. Private employees in the U.K. (and other European countries) can use Article 8 ECHR as a means of challenging abusive monitoring practices. If the employer is classified as a private employer, then the Convention gives only indirect guidance on the way courts and tribunals approach and interpret existing common law/statutory rights. The court may be asked to consider the monitoring in "light of his/her right to privacy under [Article 8 in] the HCHR."[348]

The U.K.'s chief regulatory agency, called OFTEL,[349] issued "Guidance on Recording on Private Conversations in 1999" to govern the monitoring of calls. The purpose of these guidelines was to provide businesses with safe harbor information on how to implement electronic monitoring without violating the privacy of their employees. OFTEL's

342. *Id.* at 7.

343. *Id.*

344. *Id.*

345. The Act came into force on October 2, 2000 and was enacted to implement the ECHR of 1950.

346. NICK HIGHAM & SARA ELGSTRAND, DATA PROTECTION OVERVIEW (2001).

347. *See* § 6(1) of the HRA (stating that "[i]t is unlawful for a public authority to act contrary to a Convention right" (HCHR), including employment).

348. JOANNE SAWYER, PURSUING PRIVACY AT WORK THROUGH THE HUMAN RIGHTS ACT, Liberty, U.K. (2001).

349. OFTEL was the U.K. regulator for the telecommunications industry, but has been replaced by Ofcom. Ofcom is an independent regulator and competition authority for the UK communications industries, with responsibilities across television, radio, telecommunications and wireless communications services. *See* Office of Communications, *About Ofcom*, *at* http://www.ofcom.org.uk/about_ofcom/ (last visited May 28, 2005).

document tacitly assumes that Internet access has the same protection as telephone communications under European law.[350] It is likely that courts in all European states will be more receptive to extending privacy-based rules for telephone usage to communications over the Internet, in stark contrast to American judicial decisions. Workers in the U.S. currently enjoy no reasonable expectation of privacy for e-mail communications at work because courts treat business computers as the property of the employer rather than as personal computers.[351] In contrast to the fundamental rights approach evolving in the U.K., American courts do not recognize a privacy interest in personal e-mail folders or correspondence.

b. The Regulation of Investigative Powers Act of 2000

The U.K.'s Regulation of Investigatory Powers Act 2000 (RIP Act) makes it a criminal offense to intentionally intercept, without authorization, "any communication in the course of its transmission."[352] The RIP Act makes it a criminal offense to intercept communications from any "public postal service" or "a public telecommunication system."[353] An interception is defined as any modification, interference or monitoring of electronic communications.[354] The RIP Act is inapplicable to private telecommunications systems such as intranets or Virtual Private Networks.[355] The U.K. statute contemplates public enforcement by the police, but there is no express provision for private enforcement by plaintiffs such as employees whose data has been intercepted.[356]

The RIP Act does not address the workplace scenario specifically, but permits employers in general to intercept e-mail or monitor Internet access so long as both senders and recipients consent. If law enforcement obtains a lawful warrant, the interception may be permitted under U.K. Telecommunications Regulations.[357] U.K. employers may intercept e-mail or Internet communications only if the monitoring is conducted to carry out

350. NICK HIGHAM & SARA ELGSTRAND, DATA PROTECTION OVERVIEW (2001).

351. *See, e.g.*, McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 Tex. App. LEXIS 4103 (Tex. App. 1999).

352. Regulation of Investigatory Powers Act, 2000, c. 23, § 1(1) (Eng.), *available at* http://www.hmso.gov.uk/acts/acts2000/00023a.htm (last visited May 22, 2005).

353. *Id.* at § 1(1)(a), (b).

354. *Id.* at § 2.

355. *Id.* at § 6 (noting the exclusion for "an interception of a communication in the course of its transmission by means of a private telecommunication system").

356. *Id.* at § 7(a), (b) (describing fines and imprisonment of terms not exceeding two years for unlawful interceptions).

357. Statutory Instrument 2000 No. 2699, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, *available at* http://www.hmso.gov.uk/si/si2000/20002699.htm (last visited May 22, 2005).

the employer's business activities. It would not be a business objective for a U.K. executive to intercept e-mail to learn more about the personal lives of employees. The RIP Act was enacted to ensure that interception of electronic communications was appropriately balanced with basic human rights,[358] which confirms the evolution of privacy as a fundamental human right. While no case law has yet construed the RIP Act, it is quite likely that workers will find limited protection under the statute.

c. The Lawful Business Practice Regulations

The United Kingdom's Lawful Business Practice Regulations (LBPR) govern the rights and responsibilities of businesses that monitor electronic communications.[359] The LBPR provide exceptions to the RIP Act, stating that conditions for monitoring without employees' consent. Companies may monitor and keep records of Internet communications to comply with regulatory or self-regulatory practices and procedures.[360] The monitoring of company employees must be limited to their use of the company's computer system within the scope of their duties.[361]

The LBRP authorizes interception without employees' express consent in five circumstances: (1) to establish the existence of facts, to ascertain compliance with regulatory or self-regulatory practices or procedures (quality control and training); (2) to prevent or detect crimes; (3) to investigate or detect unauthorized use of telecommunication systems; (4) to secure, or as an inherent part of, an effective system operation; and (5) to determine whether or not the communications are business communications.[362]

---

358. THE RECORD MANAGEMENT SECTION, DATA PROTECTION AND PRIVACY PRACTICE (2001), *available at* http://www.recordsmanagement.ed.ac.uk/InfoStaff/masons_newsletters/issue5.pdf.

359. Statutory Instrument 2000 No. 2699, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, *available at* http://www.hmso.gov.uk/si/si2000/20002699.htm (last visited May 22, 2005).

360. *Id.* at § 3(a)(i)(aa), (bb). An employer must not only comply with LBPR but also the Telecommunications Regulation of 1999 implementing the Data Protection Directive (97/66/EC, also refereed to as the ISDN Directive) about processing of personal data and the protection of privacy in the telecommunications sector. The Telecom Directive, which updates definitions for telecommunications services and networks with new definitions for electronic communications and services to ensure technological neutrality and update the law to encompass e-mail and use of the Internet. The Telecomm Data Directive requires the U.K. and all other Member States to protect "the confidentiality of communications made by means of public telecomm systems and specifically prohibits activities such as recording or tapping by others than users." Dept. of Trade & Indus., *Unlawful Business Practices, Response to Consultation, at* http://www.dti.gov.uk/ industries/ecommunications/lawful_business_practice_regulations__response_to_consultation.html (last visited May 22, 2005).

361. *Id.* at § 3(a)(i)(cc).

362. LBPR broadly addresses any lawful interceptions of communication and does not

However, interception is only authorized if the controller of the telecommunication system (or the employer) has made all reasonable efforts to inform potential users that the interception may take place.[363] Failure to comply with this requirement can render the use of the intercepted personal data unlawful. LBPR is only focused on business communications, which means that it does not permit employers to monitor personal communications.[364] The British approach creates a line of demarcation between e-mail that is personal or private from business and private communications.[365] If there is a reasonable suspicion that an employee is violating a corporate e-mail policy, the employer must be prepared to present evidence that led to further investigation.[366]

d. The Importance of a Clear Policy

According to the RIP Act, LBPR and DPA, only communications "in the course of transmission" may be lawfully intercepted. This might give rise to problems when it comes to stored records of private e-mails and Internet usage. To avoid this legal exposure, companies need a clearly delineated Internet or e-mail usage policy. In addition, the employer should require the employees to agree to the terms, since "the regulations expressly do not affect monitoring to which employees have given their consent."[367] A Code of Practice for both e-mail and Internet usage is the most efficient measure of ensuring the privacy and rights of the employees and protecting the employer from any potential liabilities.

D. The French Approach to E-Surveillance

The French government is concerned about how the commercialization of private information threatens the right to privacy, legislation, and fundamental freedoms, not only for individuals but also for society and democracy as a whole.[368] The French government has been

---

specifically address the monitoring of traffic data, storage, or use of personal information obtained as a result of interception. *See supra* note 359.

363. *Id.* at 26.

364. *Id.*

365. *Id.*

366. *Id.* at 8.

367. *See E-mail and Internet Monitoring: A Snooper's Charter?*, WORKING BRIEF (Henmans Newsletter Oxford, U.K.), Dec. 2000, *at* http://www.henmans.co.uk/emp_nwo8.html (2004).

368. Guy Braibant, *Données Personnelles et Société de L'information*, RAPPORT AU PREMIER MINISTRE SUR LA TRANSPOSITION EN DROIT FRANÇAIS DE LA DIRECTIVE 95/46 (Mar. 3, 1998), *available at* http://www.forumInternet.org/documents/rapports_avis/lire.phtml?id=67.

reticent in legitimating information-gathering regarding physical persons in its attempt to protect 175 citizens from privacy abuses associated with new technologies. In January 1978, the French government instituted "*La Commission Nationale de l'Informatique et des Libertés*" (National Commission for Information Technology and Civil liberties) (CNIL),[369] an independent administrative authority.[370] CNIL's main purposes are to protect *la vie privée* (the right to a private life), to propose legislation, and to inform and educate the French people about their rights regarding all aspects of electronic communication.[371]

The CNIL has a close relationship with another legal institution, "*Le Forum des droits sur l'Internet*" (FDI), which translates as the forum of the rights on the Internet, and is supported by the French government and private entities.[372] This collaborative institution functions like an incubator for the various issues that can arise in the virtual world—for example, the relationship between work and the Internet.[373] CNIL recognizes that there is an expectation among employees to be able to use the Internet at work for personal use, just as they were able to use the phone and minitel[374] for personal conversations before.

The FDI concludes that this is a reasonable trade off, because the employer benefits from having his employees connected and available via the Internet at all times.[375] In some cases this means that the employer has the ability to reach the employees at all times through portable computers and cell phones; therefore, the FDI contends that it is only fair for employees be able to use these electronic devices for some personal use as well.[376]

---

369. Through the law n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (the law about information technology).

370. This means that it does not obtain instructions from any other authority and is financed by the state.

371. *See* CNIL République Française, *L'institution*, *at* http://www.cnil.fr/index.php?id=16 (last modified Apr. 8, 2005).

372. Le Forum des droits sur l'Internet, *Ministère délégué à la Recherche et aux Nouvelles Technologies, at* http://www.droitdunet.fr/a_propos/partenaires.phtml (last visited May 25, 2005).

373. Le Forum des Droits sur l'Internet, *Groupe de Travail Relation du Travail et Internet* (Aug. 8, 2001), *at* http://www.forumInternet.org/groupes_travail/lire.phtml?id=43.

374. Minitel is a monochrome teletext system founded in 1981 and launched in 1983 by France Telecom in France. The publicly available network system made sharing information with electronic communication more efficient. James Arnold, *France's Minitel: 20 years young*, *at* http://news.bbc.co.uk/2/hi/business/3012769.stm (last updated May 14, 2005).

375. Le Forum des Droits sur L'Internet, *Relations du Travail et Internet* (Sept. 17, 2002), at 14 & 16, *available at* http://www.forumInternet.org/telechargement/documents/rapp-RTI-20020917.htm.

376. *Id.* at 12.

1. French Legislation on Internet Monitoring

As with other European countries, in France, Article 8 of the ECHR[377] and Article 9 in the Civil Code[378] regulate the right to a private life. Article 9 states that "everyone has a right to a private life, which allows a judge to take all measures possible to prevent any attempts to threaten the intimacy of the right to a private life."[379] The definition of a private life is not clearly established; it is decided on a case by case basis.[380] However, some of the basic elements of private life include secrets, sexuality, health, family, feelings and friends.[381] These are aspects of life that French society wants to protect against third-party spying and prying.[382]

An 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.[383] However, a French employer is not allowed to collect any information of a personal character unless he has clearly informed his employees about it, and the information about the monitoring is easily available.[384] If the employer does not comply with the notice requirement, he can get punished with up to three years of prison and 45,000 • in fines for knowingly intercepting personal electronic communications or even for having devices in the system that can intercept.[385] In America, monitoring without notice is not a criminal act; rather, the employer is permitted to monitor the communication systems even without any notification since the systems are the property of the employer.

A French employer is permitted to control employees' electronic

377. *See supra* Part B.2.

378. Code civil [C. CIV.] art. 9 (Fr.).

379. *Id.*

380. Guy Braibant, *Données personnelles et société de l'information*, RAPPORT AU PREMIER MINISTRE SUR LA TRANSPOSITION EN DROIT FRANÇAIS DE LA DIRECTIVE 95/46 (Mar. 3, 1998), at 6, *available at* http://www.forumInternet.org/documents/rapports_avis/lire.phtml?id=67.

381. *Id.* at 7–8.

382. Information can have both private and public character, depending on what the intention was when the information was given. Private information can be given a public character by voluntary acts: for example, addresses and phone numbers given to a phone company in order to be listed in a phonebook. Also, acts made in public or professional places maintain private information: for example, one eats and drinks in public and professional places, disclosing what it is that he is consuming, but that information will still maintain a private character. *Id.*

383. Code du travail [C. TRAV.] arts. L.120-2 & L.422-1-1 (Fr.).

384. Code du travail [C. TRAV.] arts. L.121-8, R. 122-12 & L. 412-8 (Fr.).

385. Code pénal [C. PEN.] art. 226-15 (Fr.).

communications but must protect their right to privacy.[386] The FDI recognizes that an absolute ban of private messages would be unenforceable for employees who occasionally use the Internet for personal use.[387] Further, if the employer restricts private use of electronic communications, then that restriction has to be proportional and reasonably calculated to protect the company.[388] No employer could prohibit all personal use of the corporate network, because no French court would ever view an absolute ban as a proportional measure.[389]

A network administrator can implant a surveillance system to protect against abuse, but he is only allowed to analyze web traffic or patterns of web addresses.[390] An administrator should be able to monitor whether employees are visiting pornographic web sites, or if they are transmitting other objectionable content.[391] An employer's computer system administrators may monitor general traffic, but they are not permitted to read or monitor specific messages. A systems administrator can control web traffic flow or conduct systems maintenance without prying into the specific content of messages, which would violate privacy. An administrator who crosses the line of reading specific messages may be sanctioned by fines and imprisonment.[392]

2. Online Privacy Cases

French courts have clearly articulated employees' right to online privacy in the workplace. In *Societe Nikon France v. M. Onof*,[393] the court held that an employer had no legal right to intercept and read personal e-mails, even if the employer supplied the computer and expressly provided that employees were not to use their computers for personal e-mail or

386. Le Forum des droits sur l'Internet, *Relations du travail et Internet* (Sept. 17, 2002), at 19, *available at* http://www.foruminternet.org/telechargement/documents/rapp-RTI-20020917.htm.

387. *Id.* at 17.

388. Code du travail [C. TRAV.] art. L.122-43 (Fr.).

389. *Id.* at 17.

390. *Id.* at 19.

391. The employer has no right to disturb the private life and the individual freedoms of employees, or impose restrictions that are not justified as loyal, transparent and proportional. Code du travail [C. TRAV.] art. L.120-2 (Fr.). *Relations du travail et Internet*, *supra* note 375.

392. Code pénal [C. PEN.] arts. 226-15 & 432-9 (Fr.); ECHR, *supra* note 209 (noting that the right to keep private correspondence secret has been recognized in France since 1938 (Mas et association de la critique dramatique v. de Rovera et Signorino, Cour d'Appel de Paris, 17 June 1938)).

393. Cour de Cassation [Cass. soc.], Chambre social, Oct. 2, 2001. (Cour de Cassation is the Supreme Court of France).

Internet uses.[394] The *Societe Nikon* court validated the employee's zone of privacy, finding it permissible to use the Internet for personal use during work time.[395] The court also said that the employer had no right to intercept files clearly marked as personal files.[396] The *Societe Nikon* court held that employers have no general right to monitor e-mail or Internet communications unless the employer has complied with the notice requirement.[397] In addition, it must be proven that the employee has actual knowledge of the employer's monitoring activities.[398]

A decision by the Cour d'Appel de Montpellier[399] held that the employer has the burden of proof in demonstrating that employees have been expressly informed about the surveillance of electronic communications. The court held that the employer did not comply with the notice requirement by notifying employees that Internet monitoring could be possible sometime in the future when seventeen installed 175 Internet systems in 1996.[400]

Even if the French courts are solicitous of the private lives of employees, they have upheld the termination of employees who misused of computers at work by using them as instrumentalities for crime. The court in *Marc P. v. Spot Image*[401] confirmed that the employer acted properly when it dismissed the plaintiff from work after the discovery that he had transmitted anti-Semitic e-mails from his workplace computer. The court stated that when it comes to illegal e-mail or content that is objectionable, employees have no right to offensive or criminal messages.[402] An employer transmitting illegal or objectionable e-mails is acting outside the scope of his employment and is contrary to professional norms.[403]

In France, the FDI gives guidelines on how an employer can ensure

---

394. France established very early that employees have the right to privacy when corresponding at work, which was the outcome of Mas et association de la critique dramatique v. de Rovera et Signorino, Dalloz Hebdomadaire, Cour d'Appel de Paris, 17 June 1938, p. 520.

395. When deciding this case the court looked at Article 8 of ECHR, Code civil [C. CIV.] art. 9 (Fr.) and Code du travail [C. TRAV.] art. L.120-2. (Fr.). *Id.*

396. *See* F. M., H. H. et V. R. v. Ministère public et A. T., Cour d'Appel de Paris, 17 Dec. 2001 (holding that private electronical communication is protected by Art. 432-9 in the Criminal code as "correspondence").

397. *Id.*

398. The actual knowledge requirement was also developed in two cases regarding video surveillance, *M. Alaimo v. Societe Italexpress Transports Groupe Frans Maas*, Cour de Cassation, Chambre social, 31 Jan. 2001; *see also* Societe Transports Frigorifiques Europeens v. M. Smari, Cour de Cassation, Chambre social, 15 May 2001.

399. SCP Lefevre et Broussous v. Monsieur P.K., Cour d'Appel de Montpellier, Chambre sociale, 6 June 2001.

400. *Id.*

401. Cour de Cassation, Chambre social [Cass. soc.], June 2 2004.

402. *Id.*

403. Code du travail [C. TRAV.] art. L.120-4 (Fr.). *Id.* at 3.

that it is violating an employee's right of privacy. First, employees should indicate whether the communication is private or business related; if it is not indicated, there should be a presumption that the message is business-related.[404] If the message, in fact, is private, then the administration has a duty to label it private.[405] The FDI does not support encrypted messages, since there is a great risk that the message will be classified as a virus and be quarantined.[406] Second, the firm should have some kind of Internet policy where employees are warned about the need to exercise good faith when they execute their work[407] or in the labeling of messages and files.[408] The policy should be in written form with clear and conspicuous terms and conditions. The employer must also give employees notice about their e-mail and Internet policy[409] because it is illegal for the employer to monitor the system without having first informed the employees. An employer's failure to comply with the notification procedures may be used as evidence against the employer in a subsequent proceeding.[410] Third, the employer may protect its computer system by filtering out objectionable websites or blocking the downloading of large files.[411]

Further, the FDI requires that the administrator of personal data has a duty to ensure the security and the confidentiality of information. The company's e-mail and Internet policy should warrant that an individual's confidentiality will be protected.[412] The European Commission has adopted a similar approach for its new directive on employment-specific rules on data protection at the workplace. This is also an important first step in order to maintain the privacy of employees where employers have a legitimate reason to monitor e-mails and Internet usage.

IV. REFORMING E-MAIL AND INTERNET USAGE

A. Two Different Paradigms for Workplace Privacy

American and European employers have diametrically opposed approaches to workplace privacy, as can be seen through the lens of the PhDog.com hypothetical. Part I documented the U.S. "property-rights" approach to online workplace privacy versus the European human rights approach discussed in Part II. The two different paradigms for online

404. *Id.* at 18.
405. *Id.*
406. *Id.*
407. Code du travail [C. TRAV.] art. L.120-4 (Fr.).
408. *Id.* at 21.
409. *Id.*
410. Code du travail [C. TRAV.] art. L. 121-8 (Fr.).
411. *Id.* at 19.
412. *Id.* at 20.

workplace privacy can be largely explained by the U.S. emphasis on market-driven solutions or "*savoir faire*," as opposed to the greater emphasis on human rights throughout Europe.

As we have learned from our hypothetical, employers in the United States enjoy a "duty-free" zone when it comes to electronic spying in the workplace. 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. A multinational corporation such as PhDog.com would need to audit its surveillance practice before implementing it in Europe, where the employer's ability to monitor e-mail is balanced against the employees' right to privacy. In Europe, e-mails are regarded as private communications and are accorded the same protection as phone calls whereas American courts use the private/public distinction to divest workers of any expectation of privacy.[413] America has yet to develop meaningful common law or statutory remedies, even when electronic surveillance is implemented in an arbitrary or discriminatory manner.

In general, the United States is more standard-oriented than the rule-specific regimes implemented in Europe. Every European country (with the exception of the United Kingdom) follows civil law systems that evolved out of Roman law. The predominant effect of civil codes is to forge bright-line protections, as opposed to fuzzy precedents. The civil law regimes of Europe vary substantially from country to country, but it is fair to say that the approach is more rule-oriented than in the United States. The civil code countries protect their workers using bright-line rules that prescribe what specific steps must be taken to implement electronic monitoring of workers.

In America, it has been clear that whatever is in your work computer belongs to your employer. If the employer has an e-mail and Internet policy forbidding all personal use, he can inspect any files on the computer with impunity.[414] A recent article defended these practices, contending that current U.S. law is consistent and "fair given the nature and purpose of the workplace."[415] We disagree. Electronic surveillance practices in the U.S.

---

413. *See, e.g., Ex Parte* Jackson, 96 U.S. 727 (1878); *see also* Vernars v. Young, 539 F.2d 966 (3d Cir. 1976).

414. *See* McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 Tex. App. LEXIS 4103 (Tex. App. 1999); *see also* Albert J. Muick v. Glenayre Electrics, 280 F.3d 741 (7th Cir. 2002) (describing events in which laptop used by plaintiff in the course of his employment was seized by his former employer who handed it over to the federal authorities in response to a search warrant. The court held that no privacy right was violated since the company's policy gave them the right to inspect the laptop at any time).

415. Christopher Pearson Fazekas, *1984 Is Still Fiction: Electronic Monitoring In The Workplace And U.S. Privacy Law*, 2004 DUKE L. & TECH. REV. 15 (2004), *at* http://www.law.duke.edu/journals/dltr/articles/2004dltr0015.html (last visited May 25,

workplace infringe on the fundamental privacy rights of workers and constitute the functional equivalent of a digital leash.

No current technology gives employers the software to distinguish between an employee's personal communications and her business communications. Under current U.S. law, business as well as private communications are deemed to be the personal property of employers. Further, we contend that there is a need for a *more* balanced approach in the United States. We propose an Electronic Monitoring Act of 2005 which would give all U.S. employees actual notice (written and electronic) and require their express and informed consent before any monitoring program can be implemented. The American approach to telephone calls recognizes a distinction between personal and business use, and that same logic should be extended to e-mail.

1. Market-Driven America vs. Human Rights-Oriented Europe

American employers are not hamstrung by the requirement that an employer formulate clear e-mail and Internet guidelines, inform their employees, and obtain express consent before monitoring. Throughout Europe, workers enjoy greater procedural rights protecting their basic rights to privacy in the workplace. European employers, for example, are required to give employees clear and conspicuous notice about e-mail surveillance. If actual notice of surveillance is not established, any interception of electronic communications is considered to be unlawful. In contrast, the U.S. permits employers to monitor electronic communications even if they do not have a clear policy or have not informed the employees about the surveillance. Even if a European employer restricts Internet usage and totally prohibits personal use of business computers, they are not permitted to indiscriminately read all messages and files. Courts throughout Europe require that electronic surveillance be supported by a specific "employer need to know" basis. In other words, electronic monitoring must be reasonably based, proportional, transparent and non-discriminatory.[416] If an employer fails to comply with the specific requirements, it is exposed to civil as well as criminal liability, unless the firm can demonstrate that an exception applies. This is contrary to the rights of an American employer, where courts have validated employers' monitoring of electronic communications even if the company has expressly promised not to monitor messages and has not formulated a

2005).

416. Gilbert Demez, La preuve en droit du travail: protection de la vie privée et nouvelles technologies, in Question de droit social, Formation permanente CUP series, No. 56 (2002).

specific policy.[417]

B. Towards a New Kind of Workplace

Even if the presumption is that all use of computers is for work, European courts acknowledge that employees may have private files and messages on their work computers, so long as they are clearly delineated. In contrast, U.S. courts have formulated the legal fiction that there is no such thing as a private file on an employee's office computer. In America there has been one decision where a court held that the plaintiff had a reasonable expectation of privacy in his personal AOL e-mail account, even if access was from a work computer.[418] However, the majority of courts follow *U.S. v. Charbonneau*,[419] which found no expectation of privacy in a personal e-mail account. In that case, the defendant was convicted of possessing child pornography based on images found on the defendant's office computer. Similarly, the First Circuit in *United States v. Councilman*[420] held that, irrespective of the nature of e-mails, a plaintiff had no standing to argue that the federal Wiretap Act applies, because e-mail is considered to be in storage when intercepted.[421]

In this era of information technology, where the fixed workplace is being rapidly displaced by a more protean electronic environment, wireless network connections create a seamless workplace.[422] In a telecommuting world, an employee's workplace may be anywhere and everywhere. This evolution gives employees more freedom, more time with their families, and decreases the traffic on our roads. Technology also benefits employers, who are able to communicate with their employees at all times. In order to ensure some privacy for an American employee working in a cross-border workplace, he would have to have two computers, one for private files and one for business; but this is often impractical.

Some commentators believe that the current U.S. legal regime of no privacy in the electronic workplace is appropriate because the federal

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

418. U.S. v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996) (holding that when the FBI searched through the work computer of the plaintiff, a military officer, the massages sent to another AOL subscriber were private).

419. 979 F. Supp. 1177 (S.D. Ohio 1997).

420. 373 F.3d 197, 209 (1st Cir. 2004) (reasoning that Congress intended to exclude stored communications from the scope of the Wiretap Act).

421. In October of 2004, the First Circuit withdrew its opinion in *Councilman* and granted a rehearing en banc. United States v. Councilman, 385 F.3d 793 (1st Cir. 2004).

422. Eight percent of employees in the U.K. had a portable computer through work in 2001, which were at that time the best equipped employees in Europe. Le Forum desdroits sur l'Internet, *Relations du travail et Internet* (Sept. 17, 2002), at 8, *available at* http://www.forumInternet.org/telechargement/documents/rapp-RTI-20020917.htm.

government does not provide specific protections.[423] This formalistic approach to workplace privacy rights is based upon the simple premise that employees foreclose their privacy rights when using their employer's computer network.[424]

Workers relinquish their right to privacy in the workplace whereas they enjoy heightened protection of privacy in their private residence.[425] But the rise of telecommuting has obscured the sharp divide between the private home and the workplace. If employers monitor computer usage in the home on an employer-issued computer, the employer will no longer have a zone of privacy in his residence. The European approach to electronic monitoring is to recognize a zone of privacy that applies in the workplace as well as the home. Under the European privacy-based regime, workers never waive their privacy rights, whether they are working from home or at the office. A more humanistic legal environment must recognize a zone of privacy but also validate the right to monitor where there is a demonstrated need.

C. Towards a Harmonized Safe Harbor for Electronic Monitoring

"The state of nature has a law of nature to govern it, which obliges everyone: and reason, which is that law, teaches all mankind, who will but consult it, that being all equal and independent, no one ought to harm another in his life, health, liberty, or possessions."[426]

Much ink has been spilled about the consequences of computer technologies in eroding privacy. Much of the commentary has been critical of the U.S. approach, which refuses to balance employee privacy against the employer's need to monitor. In the case of the electronic workplace, there is lag between legal norms and technology.[427]

---

423. Fazekas, *supra* note 415.

424. *See* Smyth v. Pilsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996); McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 Tex. App. LEXIS 4103 (Tex. App. 1999).

425. *See, e.g.*, Commonwealth v. Brion, 652 A.2d 287, 289 (Pa. 1994) (remarking "[f]or the right to privacy to mean anything, it must guarantee privacy to an individual in his own home" and held that the officer was not allowed to record a conversation in Brion's home even if he had consented, because there was no probable cause); Dietemann v. Time, Inc., 449 F.2d 245 (9th Cir. 1971) (holding that the plaintiff had a reasonable expectation of privacy from being secretly photographed and recorded by reporters that he had invited into his home office).

426. JOHN LOCKE, THE SECOND TREATISE OF GOVERNMENT, Ch. II, 6 (1690). John Locke (1632-1704) lived in England and his books Two Treaties on Government argue that man is born free in nature; because man is free and rational entity, he has a contract with the state in which he does not give up his inalienable rights of life, liberty and property. Should an oppressive government challenge those rights, then man should rebel.

427. *See generally* Eltis, *supra* note 18, at 487 (2003) (arguing that it is incumbent to harmonize the law as to e-mail eavesdropping in the global economy).

Briefly stated, we propose The Electronic Monitoring Act of 2005, a provision that shares common ground with a proposed federal statute introduced in the 106th Congress that languished in committee.[428] Our proposed federal statute would go beyond notice in providing meaningful remedies against the misuse or abuse of electronic surveillance. Our proposal act would require all U.S. employers to provide electronic notice of electronic surveillance to all employees and prospective employees. Employees must be advised electronically that monitoring of e-mail or Internet usage has been implemented each time they access their employer's computer system. In addition, all employers would be required to give specific written notice to employees *prior* to instituting a monitoring program. Employers who instituted clandestine monitoring programs would be deemed to be in violation of the federal statute.

Finally, all employers implementing a monitoring program would be required to articulate legitimate business reasons for instituting a monitoring program, which may include protecting intellectual property assets, reducing online torts, or other employment-related reasons. Employers instituting monitoring outside a "need to know" basis would be subject to criminal as well as civil penalties, including compensatory as well as punitive damages. Prevailing employees may also receive reimbursement for attorneys' fees and costs in the proper case. This simple right to notice and the formulation of meaningful remedies against abuses would essentially eliminate oppressive monitoring enabled by a legal environment of absolute immunity for electronic surveillance.

In the long run, our proposed federal legislation would make U.S. companies such as PhDog.com more competitive in their trade with Europe. The statute would, in effect, lower the cost of harmonizing U.S. practices with the European law of electronic monitoring. In an interconnected world where the personal data of workers crosses international borders, it is critical that European and U.S. electronic surveillance practices be more uniform. Any business transmitting data from any of the member states of the E.U. must already conform to each country's implementation of the Data Protection Directive. Consent must be obtained from the data subject prior to entering in to the contract, and this consent is vital for any processing of personal data,[429] contrary to the viewpoint of American courts where there is no need for explicit consent before processing of personal data obtained through monitoring.

Member states of the E.U. are required to provide that a transfer of personal data to other countries takes places only if there is assurance of an

428. Notice of Electronic Monitoring Act, H.R. 4908, 106th Cong. (2000).
429. *Id.* at Art. 7.

"adequate level of [data] protection."[430] All organizations are prohibited from transferring the personal information of Europeans unless the transferee complies with the Directive's notice and choice principles.[431] If a European company does not respect these principles, the company can be civilly liable for the unlawful processing of personal data.[432] Damages may be assessed for collecting or transmitting information without data subject consent,[433] which would not be the case in America where there is more or less no expectation of privacy. At present, any company such as PhDog.com transferring personally identifiable information of European workers would be in violation of the Data Protection Directive,[434] and the company would have to pay damages.

U.S. companies need to maintain a dynamic equilibrium between their business need to monitor electronic communications and the privacy rights of workers. Creating informational privacy rights for American workers is critical to the future of cross-border sales and services. The shrinking of national boundaries in our global economy creates new legal dilemmas for companies that violate European legal norms. Amazon.com, for example, has been investigated in Europe for violating data protection laws in the collection of personal data on visitors.[435] It follows that other U.S.

---

430. *Id.* at Art. 17 (in general) and Art. 25 (for other countries outside the E.U.). The six legal grounds defined in the Directive are "consent, contract, legal obligation, vital interest of the data subject or the balance between the legitimate interests of the people controlling the data and the people on whom data is held (i.e. data subjects)." European Commission Press Release: IP/95/822, *Council Definitively Adopts Directive on Protection of Personal Data* (July 25, 1995), *at* http://www.privacy.org/pi/intl_orgs/ec/dp_EC_press_ release.txt (last visited May 4, 2005).

431. U.S. Dep't of Commerce, *Safe Harbor Privacy Principles* (July 21, 2000), *available at* http://www.export.gov/safeharbor/shprinciplesfinal.htm. The European Commission approved new standard contractual clauses which business can use to ensure adequate safeguards when data is transferred from the E.U. to a non-E.U. country in Commission Decision C (2004)5271 from Jan. 7, 2005. Europa, *Data Protection: Commission Approves New Standard Clauses for Data Transfers to Non-EU Countries* (Jan. 7, 2005), *available at* http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/05/12&format=HTML&aged=0&language=EN&guiLanguage=en; EUROPEAN COMMISSION, DATA PROTECTION IN THE EUROPEAN UNION, *available at* http://europa.eu.int/comm/internal_market/privacy/modelcontracts_en.htm (last visited May 25, 2005).

432. *See id.* (providing "adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals").

433. *Id.*

434. Ann Cavoukian, *The State of Privacy and Data Protection in Canada, the European Union, Japan and Australia*, PATENTS, COPYRIGHTS, TRADEMARKS, AND LITERARY PROPERTY COURSE HANDBOOK SERIES, June 2003, *available at* http://www.ipc.on.ca/userfiles/page_attachments/state-pi.pdf (last visited May 25, 2005); PRACTISING LAW INSTITUTE, INSTITUTE ON PRIVACY LAW (4TH ANNUAL): PROTECTING YOUR CLIENT IN A SECURITY-CONSCIOUS WORLD (2003), *available at* WESTLAW, TP-ALL.

435. *See* Kathleen Fay, *Amazon.com Worldwide Operations Under Fire for Revising Privacy Policy*, 17 NO. 8 E-COMMERCE L. & STRATEGY 7 (Dec. 2000) (reporting that the

companies will be at a competitive disadvantage in Europe if they implement electronic surveillance without regard to the fundamental rights of employees.

In the late 1990s, the United States Commerce Department negotiated a "safe harbor" with the E.U. for the transfer of personal data by agreeing to adhere to reasonable precautions protecting data integrity.[436] Just as the U.S. and Europe negotiated a safe harbor for the transfer of personal data, we propose a safe harbor for privacy practices and e-mail or Internet monitoring that appropriately balances the right of employers to monitor electronic communications with fundamental human rights. The Electronic Monitoring Act of 2005 would serve as an important source of law in forging a safe harbor.

The proposed Electronic Monitoring Act of 2005 would help to correct the U.S.'s image as a country that devalues privacy in the workplace. The U.S. is widely perceived to be an insecure environment for the handling of personal data, and our business community has been placed at a competitive disadvantage because of our lackadaisical practices.[437] Few sectors of the U.S. economy have adhered to even minimal data protection principles, and the fear has been that data could no longer be transferred securely to the United States.[438] The blockage of data flow to the U.S. would be catastrophic and would endanger the global information economy.[439]

V. CONCLUSION

> Gatsby believed in the green light, the organistic future that year by year recedes before us. It eluded us then, but that's no

---

United Kingdom is being asked to enjoin Amazon.com's U.K. affiliate from violating the UK's data protection act).

436. The United States is lobbying international organizations to convince them to adopt America's self-regulatory approach to privacy. The United States is participating in the Platform for Privacy Protection (P3P), which is an industry standard developed by the World Wide Web Consortium that will enable visitors to express privacy preferences through their browsers. THIRD ANNUAL REPORT, U.S. GOVERNMENT WORKING GROUP ON ELECTRONIC COMMERCE 40 (2000). U.S. Dep't of Commerce, *Safe Harbor Privacy Principles* (July 21, 2000), *available at* http://www.export.gov/safeharbor/shprinciplesfinal.htm.

437. The European and the United States Commerce Department arrived at an agreement so that data could be transferred between American and European companies. *See EU States Endorse Negotiations with United States on Data Privacy*, 67 Int'l Trade Rep. (BNA) 2252 (Nov. 3, 1998).

438. Edmund L. Andrews, *U.S.-European Union Talks on Privacy Are Sputtering*, N.Y. TIMES, May 27, 1999, at C6.

439. The Europeans were generally satisfied with privacy protection for the personal information of medical patients.

> matter—tomorrow we will run faster, stretch out our arms farther. . . . And then one fine morning—So we beat on, boats against the current, borne back ceaselessly into the past.[440]

The World Wide Web became part of the American dream in the early 1990s. It is now impossible to imagine a workplace without bandwidth, browsers, and bytes. Today workers are accessing the Internet through their cell phones, pagers, personal digital assistants and business computers. More specifically, cyberspace is increasingly part of the modern workplace because it is the place where companies host web sites, fill orders, render professional services, and communicate electronically with subsidiaries around the globe. Companies have increased their productivity and efficiency thanks to information technology, but abuse of the Internet has led companies to monitor electronic communications to protect their rights and limit their liabilities. The U.S. property-based approach to electronic monitoring has left American workers without meaningful remedies for intrusive e-spying.

Would Dr. Eckleberg's gaze today symbolize spyware used in the twenty-first century electronic workplace?[441] Would the omniscient eyes peering out from giant yellow eyeglasses view every worker's keystroke, harvest every website visited, and monitor the contents of every computer screen? Today Dr. Eckleberg's all-encompassing eye would be replaced by an electronic gaze that treats every employee in the workplace as an object to be monitored. In a world of malevolent hackers, negligent employees and widespread corporate espionage, it is imperative that companies protect their information assets. The failure to monitor employees' e-mail or Internet usage will expose a business to catastrophic losses due to reputational, legal, and business risks stemming from the compromise of trade secrets, business plans, and other proprietary information.

The long-term impact of our modest law reform would be to make the U.S. more competitive in a global economy by harmonizing workplace monitoring law with the privacy regimes of our European trading partners. Even for U.S. companies that do not do business in Europe, the proposed statute appropriately balances the employer's need to monitor against the employee's right to a zone of privacy when it comes to sensitive health information, personal finances, intimate relationships, or other private information unrelated to the workplace.[442]

---

440. FITZGERALD, *supra* note 7, at ch. 9.

441. *See generally* Eric P. Robinson, *Big Brother or Modern Management: E-mail Monitoring in the Private Workplace*, 17 LAB. LAW 311 (2001).

442. Brian S. Conneely & Jonathon D. Farrell, *Can Employers Monitor And Read Employee E-mails,* LONG ISLAND BUS. NEWS, Aug. 2, 2002, *available at* http://www.rivkinradler.com/rivkinradler/Publications/newformat/

We, just as Mr. Gatsby, believe in the green light, the dream of the technical revolution, and have faith in the Internet and electronic communications. However, the American law of privacy "stands apart from most of the world which starts instead from the position that the right to privacy is a central tenet of human dignity."[443] Whereas the American property-rights approach leaves employees without constitutional, common law or statutory remedies, the right of European employers to monitor electronic communications is balanced against employees' informational privacy rights. It is clear that there needs to be some balance in order to keep the dream of the technological revolution and the Internet alive and not turn it into a hollow and empty shell.

The path of online electronic surveillance law should strive to balance the employers' need to know with the right of employees to maintain a zone of privacy. Arming employees with limited procedural rights will lead to employees' greater productivity, because they will have a zone of privacy. This modest reform would prevent the rage against the machine of the past from repeating itself in the age of information.

To respect a reasonable expectation of privacy in employees' electronic communications in the workplace will humanize the workplace while also protecting the employer. Our limited reform, granting workers notice and remedies for employer abuses in electronic surveillance, is only the first step in developing a labor law that truly respects the dignity of the person. Gone should be the days when American employers could secretly intercept their employees' e-mail and Internet usage.

200208conneelyfarrell.shtml

443. Lasprogata et al., *supra* note 15, at ¶ 8.