Florida Law Review

Volume 54 | Issue 2 Article 3

April 2002

# Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace

Jay P. Kesan

# CYBER-WORKING OR CYBER-SHIRKING?: A FIRST PRINCIPLES EXAMINATION OF ELECTRONIC PRIVACY IN THE WORKPLACE

*Jay P. Kesan**



---

* J.D., Ph.D., Visiting Assistant Professor of Law, Georgetown University, Fall 2001; Assistant Professor of Law, University of Illinois College of Law & the Institute of Government & Public Affairs. I am grateful to my colleague, Matt Finkin, for introducing me to this topic and sharing his insights with me. I would like to thank the following individuals—Prof. Roger Blanpain and Michele Colucci, for useful discussions on this topic and for educating me about the relevant parts of European Labor Law, and Prof. Tadashi Hanami and Ikuko Sunaoshi, for sharing the Japanese perspective with me and for hosting me at the Japan Institute of Labour. Finally, a special word of thanks to Prof. Katsuya Tamai and the Research Center for Advanced Science & Technology at the University of Tokyo for hosting me as a JSPS (Japan Society for the Promotion of Science) Fellow and Visiting Faculty during which period much of this work was done. Many thanks to Professor Tom Ginsburg for his comments on an earlier version of this paper. I would also like to thank Tom Maloney for excellent research assistance and Andres Gallo for useful discussions. A shorter version of this paper was published in the Proceedings of the Conference on "On-Line Rights for Employees in the Information Society," Nov.13-14, 2000, Brussels, Belgium Kluwer Law International, 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!"[1]

> "Secret monitoring is the merciless electronic whip that drives the fast pace of today's workplace. . . . In essence, concealed surveillance combines the worst features of 19th century factory labor relations with 20th century technology, creating an electronic sweatshop."[2]

## I. INTRODUCTION

The modern workplace is saturated with the electronic tools of e-mail and the Internet. In 2000, forty million American employees sent sixty billion e-mails.[3] At the same time, almost 250 million people worldwide used the Internet.[4] Companies have learned that the use of these tools in commerce can have a positive effect on the bottom line.[5] Yet, unrestricted use and abuse of these same tools by employees may financially harm the company's operations and may subject the company to civil and criminal liability.[6] Nevertheless, these tools cannot be altogether removed from the

1. 8e6 Technologies Advertisement, WALL ST. J., Mar. 8, 2001, at A6.

2. Robert G. Boehmer, *Artificial Monitoring and Surveillance of Employees: The Fine Line Dividing the Prudently Managed Enterprise from the Modern Sweatshop*, 41 DEPAUL L. REV. 739, 808 (1992) (quoting COMM. WORKERS OF AM. LEGIS. FACT SHEET NO. 101-2-2, SECRET MONITORING 1-2 (1990)).

3. Paul E. Hash & Christina M. Ibrahim, *E-mail, Electronic Monitoring, and Employee Privacy*, 37 S. TEX. L. REV. 893, 894 (1996).

4. Mark Ishman, Comment, *Computer Crimes and the Respondeat Superior Doctrine: Employers Beware*, 6 B.U. J. SCI. & TECH. L. 6 (2000).

5. *See, e.g.*, Amy Rogers, *You Got Mail But Your Employer Does Too: Electronic Communication and Privacy in the 21st Century Workplace*, 5 J. TECH. L. & POL'Y 1, 1-3 (Spring 2000) (listing the elimination of travel and reduced time and cost of communications as two major benefits).

6. *See id.* at 4.

workplace without losing the competitive benefits of electronic communication in their respective businesses and without adversely affecting employee morale.[7] Many businesses have chosen policies of restricting the use of e-mail and the Internet as a middle ground, and most perform electronic monitoring of some form.[8] The 2001 American Management Association (AMA) survey reports the following:

> More than three-quarters of major U.S. firms (77.7%) record and review employee communications and activities on the job, including their phone calls, e-mail, Internet connections, and computer files. The figure has doubled since 1997. . . .
>
> Additional forms of monitoring and surveillance, such as reviewing phone logs or videotaping for security purposes, bring the overall figure on electronic oversight to 82%, up from 67% just two years ago. On average, 88% of companies engaged in any such practices inform their employees of their polices.
>
> . . . .
>
> In efforts to control employee misuse or personal use of telecommunications equipment . . . 40% [of firms] block Internet connections to unauthorized or inappropriate websites (up from 29% [in 2000]).[9]

Furthermore, a comparison of the 2001 AMA survey with the 2000 survey shows the following with regard to a major use of employer monitoring—disciplining employees:

| Misuse or personal use of: | E-Mail | | Internet | |
|---|---|---|---|---|
| | 2000 | 2001 | 2000 | 2001 |
| % Reporting Discipline | | | | |
| Any | 44.8 | 54.5 | 41.9 | 51.0 |
| Dismissal | 16.0 | 18.6 | 17.4 | 20.3 |
| Formal Reprimand or Warning | 29.6 | 38.7 | 26.1 | 33.6 |
| Informal Reprimand or Warning | 22.3 | 24.8 | 19.7 | 23.0[10] |

7. *See id.* at 2.

8. Dan McIntosh, Comment, *E-monitoring@workplace.com: The Future of Communication Privacy in the Minnesota Private-Sector Workplace*, 23 HAMLINE L. REV. 539, 541 (2000).

9. 2001 AMA Survey: Workplace Monitoring & Surveillance, Summary of Key Findings, *at* http://www.amanet.org/research/pdfs/ems_short2001.pdf (last visited Jan. 21, 2002).

10. *Id.*; 2000 AMA Survey: Workplace Monitoring & Surveillance, *available at* http://www.amanet.org/research/archives.htm.

The Workplace Surveillance Project reports the following: out of a total workforce of 140 million, 40 million of whom are online, 14 million U.S. employees (10%) are under "continuous" online surveillance.[11] The 14 million estimate is composed of 6.25 million (about 4.5%) and 7.75 million (about 5.5%) employees subject to continuous e-mail and Internet monitoring respectively.[12] Additionally, the 2000 AMA survey reports that 4.6% and 9.2% of *employers* conduct continuous e-mail monitoring and Internet connection monitoring respectively.[13]

Monitoring electronic communications raises the issue of an employee's right to privacy in personal dealings at work and creates new uncertainties about whether such a right exists and the contours of that right. Employee privacy has been called "the sleeping giant of the '90s,"[14] and electronic monitoring provokes concerns similar to those raised by the monitoring of telephones, regular mail, personal conversations, and an employee's physical location within the workplace, all of which are areas where the law is more or less restrictive of employer action.[15] With respect to electronic, non-telephonic communication, the law in the United States tends to favor the interests of the employer. Thus, some form of monitoring

---

11. Andrew Schulman, *The Extent of Systematic Monitoring of Employee E-mail and Internet Use*, Privacy Foundation: Workplace Surveillance Project (citing source of research as Nielsen/Net Ratings, U.S. Bureau of Labor Statistics and Int'l Labour Org.), *at* http://www.privacyfoundation.org/workplace/technology/extent.asp (last visited Jan. 21, 2002).

12. *Id.* The Workplace Surveillance Project does not account for employees who are subject to both kinds of monitoring. *Id.*

13. 2000 AMA Survey: Workplace Monitoring & Surveillance, *supra* note 10.

14. David Neil King, Note, *Privacy Issues in the Private-Sector Workplace: Protection from Electronic Surveillance and the Emerging "Privacy Gap,"* 67 S. CAL. L. REV. 441, 441 (1994).

15. *See* MATTHEW W. FINKIN, PRIVACY IN EMPLOYMENT LAW 113-24 (BNA 1995 & Cumm. Supp. 2000) (providing a good discussion of monitoring at the workplace); *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) ("Employee privacy is considered to be the most significant workplace issue facing companies today."); 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."); Jarrod J. White, Commentary, *E-mail@work.com: Employer Monitoring of Employee E-mail*, 48 ALA. L. REV. 1079, 1079 (1997) ("[E]merging 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."); Note, *Addressing the New Hazards of the High Technology Workplace*, 104 HARV. L. REV. 1898, 1910 (1991) (hereinafter *New Hazards*) ("Use of electronic mail has lent new shape to two age-old workplace conflicts: how much access employers should have to their employees' workspace, and how much freedom employees should have to use workplace resources for their own purposes. The unique status of electronic mail as somewhere between traditional business communications, such as memos, and traditional private communications, such as personal letters and phone calls, creates a conflict that seriously threatens employee privacy interests.").

has become the favored policy of many firms, but there may exist less intrusive safeguards for employers, and the actual privacy afforded employees may be determined by the details of "e-policies," which are extensions of the corporate culture.

This Article begins by establishing the failure of statutory law or common law in the United States to guarantee a right of electronic privacy in the workplace. Unlike Europe, since we do not recognize a universal right of privacy or human dignity, it is unlikely that we will see a legally guaranteed zone of privacy in the American workplace. Proceeding on that basis, I then ask how this issue can be addressed through a market-based, contractarian framework and what principles should inform employer-employee e-policies that are typically being developed by U.S. firms. To set the stage, in Part II, I explicate the underlying concerns of employers and employees regarding access to e-mail and the Internet and electronic privacy at the workplace. Relying on insights from microeconomic, principal-agent theory, in Part III, I show that in the modern computerized workplace, the difficulty in establishing supervision and control over the agent's activities and the difficulty in controlling the flow of information to and from the firm, together with the firm's need to employ the Internet to capitalize on the enhanced efficiencies resulting from an online presence, contribute to an overall loss in the principal's (i.e., the employer's) power and lessens her ability to take effective, unilateral action against the agent. As a result, it is possible to define an incentive-compatible, benefit-maximizing contract between employers and employees based on the following principles: employee participation in defining e-policies, full disclosure of all implementation schemes pursuant to these e-policies, and employer monitoring to ensure compliance with such e-policies. Such an incentive-compatible contract is superior to other solutions based solely on self-interested behavior by either the principal or the agent. Further, it is not only a lower cost result, but it also promotes mutual trust and cultivates the development of fairness norms, thereby increasing productivity and contributing to higher profits. Finally, I discuss some specific implementation details of e-policies designed along the lines described above.

## II. THE CURRENT U.S. AND INTERNATIONAL LEGAL LANDSCAPE[16]

### A. *Constitutional Law*

Most public-sector employee workplace privacy claims rely upon Fourth Amendment protection from unreasonable search and seizure.[17] Private-sector employees are not similarly covered.[18] Though not explicitly guaranteed by the Constitution, a broad right to privacy has developed based on implicit constitutional principles.[19] Still, this right applies only to instances of government intrusion and in circumstances in which the individual has a reasonable expectation of privacy.[20] In effect, there is no federal constitutional guarantee of private employee privacy in the workplace.[21] Professor Laurence Tribe went as far as to propose a Twenty-Seventh Amendment to the Constitution to protect privacy rights from the encroachment of technological advances, but "the state action requirement would limit the practical effect of the amendment on private employers."[22]

State constitutions provide little, if any, additional protection for the employee. A number of state constitutions have an explicit guarantee of privacy,[23] but California is the only state granting constitutional privacy rights to private sector workers.[24] In addition, though not tested in the context of electronic monitoring, even California would likely support

16. This section is not an exhaustive survey of U.S. and international law regarding electronic privacy in the workplace. Instead, the section is designed to highlight the failure of U.S. law to provide for employee electronic privacy in the workplace. The applicable laws in select European countries are briefly summarized to outline alternative legal approaches to the same issue.

17. *See, e.g.*, Boehmer, *supra* note 2, at 773. The legal standard for protection is whether the employee had a subjective and reasonable expectation of privacy. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

18. Kevin J. Conlon, *Privacy in the Workplace*, 72 CHI.-KENT L. REV. 285, 285 (1996) ("The [Supreme] Court has been reluctant to find state action in the private sector . . . ."). *But cf.* Boehmer, *supra* note 2, at 768 (suggesting that present-day corporate America threatens privacy more than government).

19. *See, e.g.*, King, *supra* note 14, at 442.

20. Kevin J. Baum, Comment, *E-mail in the Workplace and the Right of Privacy*, 42 VILL. L. REV. 1011, 1018 (1997); *cf. generally* Griswold v. Connecticut, 381 U.S. 479 (1965).

21. *See, e.g.*, Jonathan J. Green, Note, *Electronic Monitoring in the Workplace: The Need for Standards*, 52 GEO. WASH. L. REV. 438, 441 (1984) ("Although protection under the first and fourth amendments is available to governmental employees, courts have been reluctant to find the requisite 'state action' in the private sector, where the vast majority of workers are employed.").

22. S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace*, 32 GA. L. REV. 825, 862-63 (1998).

23. *See, e.g.*, Larry O. Natt Gantt, II, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J.L. & TECH. 345, 389 (1995).

24. Lee, *supra* note 15, at 150. California requires an employer to demonstrate a compelling interest in invading an employee's privacy. *Id.*; Conlon, *supra* note 18, at 286.

employer surveillance.[25] An employee is left then with statutory, common, or contract law for protection against unwanted invasion of privacy at the hands of the employer.[26] Though not directly applicable, the Fourth Amendment provides courts a useful framework for analyzing private-sector workplace privacy disputes, whether founded in statutes or in common law.[27] The overarching issue again is whether the employee has a reasonable expectation of privacy in the circumstances.[28]

### B. *Federal Law*

"The only federal law currently applicable to the issue of workplace e-mail monitoring is the Electronic Communications Privacy Act of 1986 [(ECPA)]."[29] "ECPA is an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968[30] [(Title III)], also known as the Federal Wiretap Law."[31] The ECPA has two important branches: the Title I[32] prohibition against the interception of wire, oral, and electronic communications and the Title II[33] prohibition against accessing stored communications.[34] Though the ECPA does not explicitly cover e-mail, the addition of electronic communications wherever Title III covers for wire and oral communications is normally interpreted to encompass e-mail.[35] However, "whom" the ECPA protects "from whom" is less settled and often debated.[36]

---

25. *See* Conlon, *supra* note 18, at 287.

26. *Id.* at 286.

27. *See* Boehmer, *supra* note 2, at 773-74. *But see* Steven B. Winters, *Do Not Fold, Spindle or Mutilate: An Examination of Workplace Privacy in Electronic Mail*, 1 S. CAL. INTERDISC. L.J. 85, 96-97 (1992) (accusing the Supreme Court of neglecting the goals of the judicial balancing test with respect to privacy in the workplace through misinterpretation of society's privacy values based "on an outdated view of both the workplace and privacy generally").

28. Boehmer, *supra* note 2, at 774.

29. Peter Schnaitman, *Building a Community Through Workplace E-mail: The New Privacy Frontier*, 5 MICH. TELECOMM. & TECH. L. REV. 177, 184 (1998-99).

30. Pub. L. No. 90-351, §§ 801-804, 82 Stat. 197, 211-25 (1968) (codified as amended at 18 U.S.C. §§ 2510-2522 (1994) and 47 U.S.C. § 605 (1994)).

31. Schnaitman, *supra* note 29, at 184.

32. 18 U.S.C. §§ 2510-2521 (2000).

33. 18 U.S.C. §§ 2701-2711 (2000).

34. Schnaitman, *supra* note 29, at 184-85.

35. *See, e.g.*, Alexander I. Rodriguez, Comment, *All Bark, No Byte: Employee E-mail Privacy Rights in the Private Sector Workplace*, 47 EMORY L.J. 1439, 1449 (1998) (explaining that judicial decisions have interpreted the zone created by the ECPA to include e-mail).

36. *Compare* Kevin P. Kopp, Comment, *Electronic Communications in the Workplace: E-mail Monitoring and the Right of Privacy*, 8 SETON HALL CONST. L.J. 861, 868 (1998) (discussing how ECPA was enacted in "response to Congress' perception that abuses associated with new technologies pose a substantial risk to civil liberties"), *with* Natt Gantt, *supra* note 23, at 352 ("Congress was primarily concerned about protecting corporations against their competitors that

"Although the ECPA would seem to protect workers from many types of electronic monitoring, including [e]-mail interceptions, the law is not clear with respect to the workplace, plus it contains some exceptions that courts may determine exclude employee protection in certain respects."[37] Title II contains "provider" and "user" exceptions (Title II exceptions).[38] Likewise, three Title III exceptions are preserved by Title I:[39] the "business use" exception,[40] the "provider" exception,[41] and the "consent" exception (Title III exceptions).[42] Since e-mail can only be truly intercepted at the moment between which it is transmitted and received, most employers monitor stored e-mail communications and the Title II exceptions control.[43] Under this caveat, each Title's exception is discussed in turn.

The Title II provider exception exempts the "provider" of a communications service,[44] though it is unclear what a "provider" is.[45] A broad interpretation of "provider" allows any private employer with a computer or network that stores e-mail to access the same.[46] Thus, Title II may trump any privacy granted to employees for their transmitted e-mail since the employer may simply make and access a backup copy.[47] Yet, some commentators warn that a narrow interpretation may not cover businesses that subscribe to a common carrier for e-mail.[48] Though not tested in the context of e-mail, the Title II user exception may be viewed as analogous to the Title III consent exception.[49]

An employee may release an employer from liability under Title III by consenting to monitoring, "unless such communication is intercepted for

---

might desire to steal valuable electronic information.").

37. Hash & Ibrahim, *supra* note 3, at 898.

38. Baum, *supra* note 20, at 1023.

39. 18 U.S.C. §§ 2510-2521 (2000).

40. *Id.* The business use exception is also known as "business extension" or "ordinary course of business" exception. *See, e.g.*, Rodriguez, *supra* note 35, at 1450.

41. 18 U.S.C. § 2511(2)(a)(i) (2000).

42. *Id.* § 2511(2)(d); *see also* Jared D. Beeson, *Cyberprivacy on the Corporate Intranet: Does the Law Allow Private-Sector Employers to Read Their Employee's E-mail?*, 20 U. HAW. L. REV. 165, 172-207 (1998) (theorizing how the exceptions apply to e-mail in light of the policies informing judicial interpretation); Kopp, *supra* note 36, at 868 (discussing the exceptions).

43. Schnaitman, *supra* note 29, at 187; *see also* White, *supra* note 15, at 1083.

44. 18 U.S.C. § 2701(c)(1) (2000).

45. *See, e.g.*, Baum, *supra* note 20, at 1024.

46. *Id.*; *see also* Beeson, *supra* note 42, at 188 (concluding, from *Bohach v. City of Reno*, 932 F. Supp. 1232 (D. Nev. 1996), that employers have broad powers to access e-mail stored on systems which they provide); Hash & Ibrahim, *supra* note 3, at 906.

47. *See* Natt Gantt, *supra* note 23, at 359-60 ("This interpretation gives employers who provide their company E-mail networks almost 'unfettered discretion' to read and disclose the contents of even their employees' personal [e]-mail messages."). *But see* Beeson, *supra* note 42, at 197-99 (questioning whether Congress intended this "bizarre result").

48. *See* Beeson, *supra* note 42, at 199-200; *see also* Baum, *supra* note 20, at 1024.

49. *See* Baum, *supra* note 20, at 1025 n.70.

the purpose of committing any criminal or tortious act."[50] Though consent may be found circumstantially, courts "have been reluctant to find such 'implied consent.'"[51] The extent to which a court will imply consent was explored in the seminal case of *Watkins v. L.M. Berry & Co.*[52] The court reasoned that "knowledge of the capability of monitoring alone cannot be considered implied consent."[53] Employers should use *Watkins* and similar holdings as reason enough to implement a policy regarding e-mail monitoring because "[w]ritten policies may support implied consent to monitoring, at least within the terms of the policy."[54]

Title III also contains a provider exception,[55] which places limitations, without analogy in the Title II exception, upon the purpose for which communications may be intercepted.[56] Directed toward protecting a service provider's normal operations and property, this exception only exempts an employer's interception "incident to the rendition of the company's services or when the company reasonably believes that the monitoring is necessary to protect its rights or property."[57] Thus, it is not difficult for an employer to fall within the "normal course of employment" exception, considering that it can meet these provisions by showing, for example, that its interception was to protect property (e.g., improper uses or theft) or to provide the service (e.g., quality checks). Though easy to establish justification, one commentator states that courts are likely to allow employer-providers to monitor, but only when employing the least intrusive means possible.[58]

Finally, Title III provides a business use exception.[59] Specifically, the ECPA exempts certain standard apparatus from its definition of "electronic, mechanical, or other device."[60] Courts have advanced two distinct approaches to the business use exception.[61] The first, termed the

---

50. 18 U.S.C. § 2511(2)(d) (2000). Title II also implicitly exempts consensual access to stored communications by prohibiting only unauthorized access. *See* 18 U.S.C. § 2701(a)(1) (2000).

51. Hash & Ibrahim, *supra* note 3, at 900. Consent will not be "cavalierly implied." Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983).

52. 704 F.2d 577, 581-82 (11th Cir. 1983).

53. *Id.* at 581 (emphasis omitted).

54. Hash & Ibrahim, *supra* note 3, at 900.

55. *See* 18 U.S.C. § 2511(2)(a)(i) (2000). Note, however, that this section expands upon the Title II definition of communications provider to include "an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication." *Id.*

56. *See id.*

57. Beeson, *supra* note 42, at 189.

58. *Id.* at 192-94. For example, a company worried about e-mail security could employ a "firewall" rather than monitor the content of e-mail messages. *Id.*

59. 18 U.S.C. § 2510(5) (2000).

60. *See* Natt Gantt, *supra* note 23, at 365-66.

61. Beeson, *supra* note 42, at 176.

content approach, emphasizes the nature of the communication.[62] Considering phone communication, courts have established the rule that an employer may monitor business-related calls, but may only monitor personal calls to the extent necessary to determine their nature.[63] Further, the court in *Epps v. St. Mary's Hospital, Inc.*[64] indicated that a communication may be considered business-related if it concerns the operation of the business or other matters in which an employer has a legal interest.[65] The second, termed the context approach, "focuses on whether the employer has a legitimate business interest justifying the interception."[66] The latest context cases employ a two-pronged analysis: whether the monitoring equipment was from the service provider or connected to the line by the subscriber and whether the interception was conducted in the ordinary course of business.[67] Applying the first prong to e-mail, an employer's successful exemption may depend on whether it qualifies as a system provider.[68]

There is a "balancing process implicit in both the content and context approaches [which] parallels the balancing of interests and limitation of scope present in both tort and Fourth Amendment privacy analysis."[69] Under the content approach, courts "decide the legitimacy of the employer's interest . . . by analyzing the purposes behind the monitoring and whether the content of the communication is reasonably related to the proffered purposes."[70] Under the context approach, courts "determine the reasonableness of the employee's expectations . . . by analyzing the employer's notification procedures."[71]

Critics of the ECPA are legion. In one way or another, many critics cite the failure of the ECPA to protect employees from employer monitoring.[72] The types of protected communications are limited. ECPA storage protection is limited, and employers may escape the ECPA under the Title II provider exception.[73] Also, neither the ECPA nor any other federal law protects "transactional" information such as the sender, recipient, and subject lines of e-mail.[74] Once an employer meets an exception, the ECPA

62. *Id.* at 176-77.
63. *See* Watkins v. L.M. Berry & Co., 704 F.2d 577, 581-83 (11th Cir. 1983).
64. 802 F.2d 412 (11th Cir. 1986).
65. *Id.* at 416-17; *see also* Beeson, *supra* note 42, at 179.
66. Beeson, *supra* note 42, at 179-80.
67. *Id.* at 180.
68. White, *supra* note 15, at 1086-87.
69. Natt Gantt, *supra* note 23, at 372.
70. *Id.*
71. *Id.*
72. *See* Wilborn, *supra* note 22, at 851.
73. *See* Rothstein, supra note 15, at 403.
74. *See* Joel R. Reidenberg & Francoise Gamet-Pol, *The Fundamental Role of Privacy and*

places no restrictions on the manner and extent of monitoring, nor does it require that an employer notify employees of monitoring.[75] In sum, the ECPA is ineffective in regulating the employer/employee relationship.[76] "As a general matter, most commentators agree that, in view of the breadth of the exceptions and provided that companies adopt comprehensive e-mail policies, it will be difficult for employees to obtain recourse against their employers under the ECPA."[77] "Without a definitive answer at this time as to the scope of monitoring allowed by the ECPA, the best approach for an employer is to develop and publish a policy regarding e-mail monitoring and get employee acknowledgment and consent to that policy."[78]

Multiple bills appeared in Congress in the early 1990s to address the perceived gaps in employee electronic privacy, but none was ever enacted into law.[79] The Privacy for Consumers and Workers Act[80] (PCWA), introduced by former Senator Paul Simon, is representative of the various bills that were considered.[81] It was intended to constrain the broad exceptions granted to businesses by the ECPA.[82] The single most important element shared by the bills was an employer's responsibility to notify employees of the details of its electronic monitoring programs.[83] Businesses, especially small operations,[84] were strongly opposed to the notice requirement due to its cost and interference with their monitoring duties.[85] Other common elements were expanded definitions of "employer"

---

*Confidence in the Network*, 30 WAKE FOREST L. REV. 105, 115 (1995).

75. Christopher S. Miller & Brian D. Poe, *Employment Law Implications in the Control and Monitoring of E-mail Systems*, 6 U. MIAMI BUS. L.J. 95, 101 (1997).

76. *See* Susan Ellen Bindler, Note, *Peek and Spy: A Proposal for Federal Regulation of Electronic Monitoring in the Work Place*, 70 WASH. U. L.Q. 853, 871-75 (1992).

77. Peter Brown, *Policies for Corporate Internet and E-mail Use*, *in* THIRD ANNUAL INTERNET LAW INSTITUTE 648 (PLI Patents, Copyrights, Trademarks, and Literary Property Course, Handbook Series No. GO-0015, 1999).

78. George B. Trubow, *Constitution v. Cyberspace: Has the First Amendment Met Its Match?*, 5 BUS. L. TODAY 41, 41 (Mar./Apr. 1996); *see also* Beeson, *supra* note 42, at 207-09 (criticizing the ECPA and suggested legislative reform).

79. Donald R. McCartney, Comment, *Electronic Surveillance and the Resulting Loss of Privacy in the Workplace*, 62 U. MO. KAN. CITY L. REV. 859, 882 (1994).

80. S. 984, 103d Cong. § 1 (1993).

81. Boehmer, *supra* note 2, at 807.

82. McCartney, *supra* note 79, at 886.

83. *Id.* at 883. Notice must be given to all parties to a communication (including third parties) and applies both to the intent to monitor and to signaling when monitoring is occurring. Bindler, *supra* note 76, at 867-68. An exception to the notice requirement was available to employers who suspected an employee of engaging in an "unlawful activity, willful gross misconduct," or conduct adversely affecting the business. Lee, *supra* note 15, at 168.

84. *See* Lee, *supra* note 15, at 169.

85. King, *supra* note 14, at 473; *see also* Julie A. Flanagan, Note, *Restricting Electronic Monitoring in the Private Workplace*, 43 DUKE L.J. 1256, 1275 (1994) (ascribing to businesses the

and "employee," periodic warning while monitoring, employee right to access monitoring records, restrictions on monitoring to performance-related information, and limitations on use and disclosure of personal data.[86] The largest benefit to workers who are surreptitiously monitored by their bosses would have been the notice requirement.[87] Another major benefit was the near-universal ban on continuous monitoring.[88] But, the PCWA had detractors, mainly from the business world. Businesses objected to the proposed act's restrictions on their ability to assess information from monitoring or to use that information to reward or punish their employees.[89] At the extreme, businesses also feared that they would lose their best weapon against employee computer crime.[90] Lamenting the lack of recognition of a right to privacy, one commentator adds, "[t]he biggest problem with the proposed Act is not the fact that it fails to accomplish its purpose, but that it represents yet another Act that attempts to deal with manifestations of the problem without confronting the underlying cause of the problem[:]" the lack of an underlying, affirmative employee right to privacy.[91]

Academics, students, and practitioners have responded with numerous legislative proposals to expand employee privacy rights. Some proposals are broad, encompassing a number of recurring themes. One commentator, mirroring the PCWA, outlines the elements which an ideal statute should contain: monitoring is limited to the workplace and not permitted in private areas, continuous and secret monitoring is prohibited, those monitored should be given notice while monitoring is occurring and should be given access to the resulting information, monitoring should be limited to legitimate business purposes and to information relevant to the job, and employers should be restricted as to their use of monitoring data.[92] Other commentators support a Fourth Amendment reasonableness framework requiring a "legitimate business purpose," the "least intrusive means possible," and notice from the employer.[93] Finding its genesis in the

---

complaint that restrictions on monitoring would hurt productivity and competitiveness with other nations).

86. Boehmer, *supra* note 2, at 808-11.

87. *See* McCartney, *supra* note 79, at 885-86.

88. *See id.* at 885.

89. *See* Bindler, *supra* note 76, at 879-80; *see also* McCartney, *supra* note 79, at 887.

90. *See* McCartney, *supra* note 79, at 887.

91. *Id.* at 890-91.

92. Conlon, *supra* note 18, at 295.

93. Lee, *supra* note 15, at 172; Wilborn, *supra* note 22, at 852-53; *see also* Boehmer, *supra* note 2, at 813 (removing the requirement of business purpose/interest and leaving a solution granting "due process in the private sector"); *cf.* Natt Gantt, *supra* note 23, at 416-17 (instituting a "compelling business interest" test, while retaining a traditional balancing test for "transactional information"). *But cf.* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy*

bargaining freedom traditionally allotted to employment relationships, another proposal is built around an affirmative, yet alienable, employee right to privacy in the workplace.[94] Thus, a presumption exists, subject to rebuttal by evidence of a bargain or by a compelling business interest, that the employee has not waived privacy rights.[95]

### C. *State Law*[96]

"The ECPA permits states to enact their own laws governing privacy as long as those laws are at least as protective of privacy as the ECPA. Most states have adopted the language of the ECPA with only minor modifications, but a few state privacy laws provide even greater protection."[97] New York and Massachusetts have similar statutes that generally prohibit employer eavesdropping and recording of spoken employee conversations in the workplace,[98] but a court, in *Restuccia v. Burk Technology, Inc.*,[99] held that the Massachusetts statute did not apply to electronic communications.[100] Connecticut law requires that employers inform employees of the existence and types of electronic monitoring but exempts monitoring common areas for security and when the employer has reasonable grounds to believe that an employee is creating a hostile environment or is violating the law or the employer's legal rights.[101] Connecticut may please advocates of employee rights, but fashioning accepted solutions at the state level is fundamentally unlikely.[102] Differing across jurisdictions in their nature and enforcement, state laws lack the uniformity of federal law. Additionally, state law is ill-suited for regulating a technology which erases state and national borders.[103] Furthermore,

---

*(What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 24-25 (taking exception to Professor Lawrence Lessig's removal, from the definition of "monitoring," of "the concern that technology allows organizations to exercise control over the actions of individuals" and finding Lessig's resulting solution, based on disclosure and minimal burden, to be lacking).

94. Rodriguez, *supra* note 35, at 1467-69.

95. *Id.* at 1468-69

96. *See* Rothstein, *supra* note 15, at 404-05 (providing a breakdown of the degree of protections afforded from state to state).

97. Brown, *supra* note 77, at 651.

98. *See id.* at 651-52.

99. No. 95-2125, 1996 Mass. Super. LEXIS 367 (Mass. Super. Ct., Middlesex County, Aug. 12, 1996).

100. *Id.* at *4-6; Brown, *supra* note 77, at 637, 651-52.

101. Brown, *supra* note 77, at 652-53; *see* Hall Adams, III et al., *E-mail Monitoring in the Workplace: The Good, the Bad and the Ugly*, 67 DEF. COUNS. J. 32, 41 (2000) (listing of state statutes addressing the interception of electronic communications).

102. *But see* Steven Winters, *The New Privacy Interest: Electronic Mail in the Workplace*, 8 HIGH TECH. L.J. 197, 223 (1992) (predicting that California law in this area will be widely adopted).

103. *See* Rothstein, *supra* note 15, at 404-05 (hinting that a state cannot reach those who intercept a communication outside of the state).

legislation with regard to workplace privacy regulation sometimes faces overwhelming resistance from corporate lobbyists.[104]

### D. *Common Law*

The historical legal enforcement of privacy rights is based on claims sounding in tort.[105] "In fact, the privacy right outlined by Brandeis and Warren in their famous 1890 law review article came to be known as the 'American Tort.'"[106] As a general rule, tort cases turn on the employees' expectation of privacy.[107] An employee wishing to sue an employer for invasion of privacy in the workplace may turn to the tort theories of intentional infliction of emotional distress and privacy torts.[108] It is highly unlikely that an employer's monitoring of e-mail would be found to rise to the level of "extreme and outrageous conduct" as required by most courts for actionable intentional infliction of emotional distress.[109] This leaves privacy torts.

Privacy torts comprise four separate causes of action: (1) intrusion into seclusion; (2) public disclosure of private or embarrassing facts; (3) false light; and (4) appropriation of another's identity.[110] Intrusion claims are the most applicable to e-mail in the workplace.[111] An intrusion into seclusion claim has three prima facie elements: (1) an intrusion; (2) that is highly offensive; and (3) the employee had a reasonable expectation of privacy.[112] "Courts generally consider electronic surveillance . . . an 'intrusion' sufficient to establish the first element of a prima facie case."[113] The second element, proving electronic monitoring to be highly offensive, is difficult because it does not involve a physical invasion.[114] Regardless, the line between the second and third elements has blurred.[115] Therefore, the

---

104. *See, e.g.*, Lee, *supra* note 15, at 160.

105. Rotenberg, *supra* note 93, at 26.

106. The European Union Data Directive and Privacy: Before the House Committee on International Relations (May 7, 1998) (statement of Marc Rotenberg, Director, Electronic Privacy Information Center and Adjunct Professor, Georgetown University Law Center), *available at* http://www.epic.org/privacy/intl/rotenberg-eu-testimony-598.html (last visited on Nov. 13, 2001).

107. *See* Adams et al., *supra* note 101, at 44.

108. *See* Baum, *supra* note 20, at 1021; *see also* Conlon, *supra* note 18, at 289-90.

109. Baum, *supra* note 20, at 1021; *cf.* King, *supra* note 14, at 457-58 (suggesting that a successful approach may be to generalize the claim to the extent that the invasion claimed is similar to that in a sexual harassment claim).

110. *See* Conlon, *supra* note 18, at 289-90.

111. Lee, *supra* note 15, at 163.

112. Conlon, *supra* note 18, at 290. "The elements of the tort are similar to the standards used in determining a Fourth Amendment claim in the public sector." Natt Gantt, *supra* note 23, at 375.

113. Natt Gantt, *supra* note 23, at 375.

114. Conlon, *supra* note 18, at 290.

115. *See, e.g.*, Lee, *supra* note 15, at 163.

outcome of a privacy claim typically turns on the employees' expectation of privacy.[116]

"In practice, courts will first define the scope of an employee's reasonable expectation of privacy and then balance the employer's business interest against the employee's individual rights."[117] Courts treat the workplace environment, the reason for the intrusion, and the means employed as factors to be considered.[118] Ultimately, by communicating an electronic monitoring policy, the employer can establish the level of privacy that employees may reasonably expect.[119] In addition, employers should certainly be able to provide enough legitimate business interests to justify electronic monitoring.[120] An employee is not likely to succeed if the employer obtained information through the employer's own computer system.[121] Sure enough, "[e]ven employees in states that recognize a common-law cause of action for invasion of privacy have met with little success in the context of e-mail monitoring."[122] In dismissing an employee action in *Bourke v. Nissan Motor Corp.*,[123] the court held that employees had no expectation of privacy, especially since they had "acknowledged and agreed to the employer's policies providing that use of its computers was for business purposes only." The employees also acknowledged that they were aware that their e-mail messages were subject to monitoring.[124] A more surprising result was a Pennsylvania court's dismissal of a claim in *Smyth v. Pillsbury Co.*[125]

> The court in *Smyth* rejected the employee's claim that his termination violated "public policy which precludes an employer from terminating an employee in violation of an employee's right to privacy" under state common law. The court also found that by voluntarily communicating allegedly unprofessional comments to a second person over the corporate e-mail system, the plaintiff lost any reasonable expectation of privacy, notwithstanding any assurances that such communications would not be intercepted by management. The court further held that, even if the plaintiff had a reasonable expectation of privacy in the context of his

116. Adams et al., *supra* note 101, at 44.

117. Conlon, *supra* note 18, at 290.

118. Lois R. Witt, Comment, *Terminally Nosy: Are Employers Free to Access Our Electronic Mail?*, 96 DICK. L. REV. 545, 565 (1992).

119. Conlon, *supra* note 18, at 290.

120. *See id.*

121. Baum, *supra* note 20, at 1011, 1020-21.

122. Brown, *supra* note 77, at 654.

123. No. YC-003979, slip. op. (Cal. Ct. App. June 1993).

124. Brown, *supra* note 77, at 654.

125. 914 F. Supp. 97 (E.D. Pa. 1996).

> messages, "the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in these comments."[126]

At common law, then, an employer may insulate itself from liability by informing employees of a monitoring program. An employer may even escape liability in the absence of any notification. And, as an example of the variability in outcomes among the states, *Smyth* indicates that employees may not even have the right to electronic privacy when affirmatively assured by their employer that personal communications will be kept private.[127] Common law has been cited as a good forum for workplace privacy reform in the absence of legislation.[128] However, courts have been hesitant to put forth the requisite amount of judicial activism to make a substantive change.[129] Besides, the cost of litigation keeps many cases from reaching an active judge,[130] and the resulting patchwork of laws also would lack the desired uniformity.[131]

### E. *The Failure of Law to Provide a Solution in the United States*

As many technologies speed past the law in general, the particular technologies enabling electronic monitoring in the workplace have outpaced the legislature's ability to react with a reasoned solution reflective of society's values.[132] Likewise, the common law is so entrenched in legal precedent, which inadequately corresponds to the reality of the "wired" worksite, that it has not been able to respond in a timely fashion either.[133] Commentators explain the current tension

---

126. Brown, *supra* note 77, at 655.

127. *See id.*

128. Wilborn, *supra* note 22, at 854.

129. *Id.*

130. *New Hazards*, *supra* note 15, at 1915.

131. Wilborn, *supra* note 22, at 855.

132. Conlon, *supra* note 18, at 285 ("The rapid growth of workplace monitoring and surveillance technology has far outpaced the development of laws that protect worker privacy interests.").

133. Winters, *supra* note 27, at 93-94. Since "cyberspace" is difficult to experience through the five senses, it is difficult to expand established laws that dealt with physical privacy to cover electronic privacy. *Id.* Furthermore, although not confined to privacy in the workplace, a recent article by Paul Schwartz explains how the tort law is a flawed scheme for policy protection on the Internet. Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1669-70 (1999). An excerpt reads:

> The necessary consensus about how community members process and share personal data in cyberspace cannot be left to emerge slowly over time through the tools of tort law and the push and pull of litigants, judges, and juries. This Article

as springing from a temporal gap, representing the lag between the issues introduced by electronic monitoring and the response to those issues by the legislatures.[134]

Electronic monitoring is an unprecedented phenomenon, giving the employer an ability to monitor practically every detail of its employees' workdays at an almost negligible cost. As employers use this capability, for legitimate and illegitimate purposes alike, one consequence is that some employees experience additional stress and suffer new indignities. But another, more subtle, consequence has been the revelation of a legal reality which is distasteful to many: that there is no independent right to privacy in the workplace. Therefore, employers have traditionally been able to reasonably (even secretly) monitor employees. Technological advances precipitated federal legislation in the form of ECPA; yet ECPA's statutory ambiguities and Congress's unclear intent vis-à-vis the employment relationship have left corporate America with plenty of room to electronically monitor employees, even without notice. With notice, employees are still exposed to electronic monitoring with very few limitations. However, the present situation is understandable in light of the

---

> has already suggested two problems with privacy-control that also speak to the weaknesses of Post's reliance on tort litigation. First, the discussion of an "autonomy trap" indicated that the use of personal data itself helps set the terms under which we participate in social and political life and the meaning we give to information-control. As a result, what is "reasonable" privacy and "highly offensive" information use is not exogenous to social trends regarding data processing, but rather is likely to reflect closely that which already takes place....
>
> Second, the Article pointed to the "data seclusion deception" regarding the rejection of personal claims for information isolation in favor of the demands of outside organizations. It argued that courts and academics predictably will favor collective demands for disclosure over privacy interests framed as an individual right of control....
>
> These two issues suggest that, given only general privacy tort standards, judges and juries will create a stable but bad equilibrium about personal data use. Indeed, as a threshold matter, the common law privacy tort will generate adequate privacy norms through litigation self-help only when the law provides sufficient incentives for plaintiffs to bring their claims to court. The incentives for this volume of tort privacy litigation are not now in place....

*Id.*

134. *See, e.g.*, Winters, *supra* note 27, at 130. *But see* The European Union Data Directive and Privacy: Before the House Committee on International Relations (May 7, 1998) (statement of Marc Rotenberg, Director, Electronic Privacy Information Center and Adjunct Professor, Georgetown University Law Center), *available at* http://www.epic.org/privacy/intl/rotenberg-eu-testimony-598.html (last visited on Nov. 13, 2001) ("Privacy as a legal right is well established in the United States, and the United States has passed many privacy laws in response to new technologies.").

traditional scope of government regulation and of the evolution of the concept of privacy in this country.[135]

"The American legal tradition eschews a powerful state role in society and draws on a deep-seated philosophy of limited government . . . . Even in the wake of increases in government regulation following the New Deal and Progressive Eras, U.S. law-making rhetoric remained hostile toward the regulation of industry."[136] Privacy is hard to pin down, but that has not hindered the creation of a wide variety of definitions.[137] American notions of privacy are historically reflected in the concept of "rugged individualism."[138] Privacy has been deemed to be akin to personal property.[139] Individual autonomy and liberty are prized,[140] and no corresponding debt is owed to the community.[141] Accordingly, the doctrine of at-will employment is founded upon the right of autonomous parties to contract freely. During the course of bargaining, each side may exchange, as consideration, tangible and intangible items that are alienable. In our system of employment, we can trade our privacy as though it were something we individually own.[142] It is the alienability of privacy that allows courts to consider the issues of consent and reasonable expectation of privacy to be controlling. It is the alienability of privacy that allows an employer to receive implied consent or to virtually eliminate any reasonable expectation of privacy by notifying its employees of a monitoring policy.[143] It is presumed that an employee in such a situation has accepted monitoring in exchange for continued employment.[144] Proposals to alter the employment-at-will doctrine through a public policy exception for privacy fail as a result of the notion that privacy belongs to

135. *But see* Rotenberg, *supra* note 93, at 27 (attacking the argument that government legislation and protection of privacy rights is "inconsistent with an American tradition" and attributing the notion of such an American tradition to lobbyists).

136. Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 EMORY L.J. 911, 921 (1996).

137. *See generally* Natt Gantt, *supra* note 23, at 411-15 (comparing Bloustein and Prosser); Pauline T. Kim, *Privacy Rights, Public Policy, and the Employment Relationship*, 57 OHIO ST. L.J. 671, 682-720 (1996) (applying concepts of privacy to tort law and to the workplace); King, *supra* note 14, at 444-46 (discussing Flaherty and Gavison); Schnaitman, *supra* note 29, at 181-82 (discussing Cate and Post).

138. Wilborn, *supra* note 22, at 834.

139. Rothstein, *supra* note 15, at 381.

140. *See* Wilborn, *supra* note 22, at 834.

141. Rothstein, *supra* note 15, at 382.

142. *See generally id.* at 381-83.

143. *See generally id.* at 382-83.

144. *See generally id.*

an individual.[145] The net result is that none of the traditional sources of American law guarantees employee privacy in the workplace.

As we will see in the next section, American law in this area is diametrically opposite to the situation in Europe. American law stands apart from most of the world, which starts instead from the concept of dignity.[146] Our concept of privacy is not shared by most cultures; some do not even have a word for privacy.[147] Like privacy, human dignity can be viewed conceptually as a fundamental right.[148] But, unlike privacy, dignity is not generated from the individual.[149] It is created by one's community and bestowed upon the individual.[150] It cannot be bartered away.[151] In societies with an operable legal right to dignity, the legal system, to various extents, has already established lines that employers may not cross with respect to monitoring.[152]

### F. *Alternative Examples from Europe*

In Europe, the regulation of privacy in the workplace generally draws from one or more of the following sources of authority: labor law, regulation of data collection and dissemination, and the protection of personal communications. For example, the United Kingdom provides a regulatory regime not far removed from that of the United States, though British employers are now subject to statutory limitations upon collection of personal data on their employees. In the following examples, I do not attempt to exhaustively review the law and regulation of privacy in the workplace in Europe. Rather, I simply outline the legal sources for workplace privacy protection in four countries in Europe.

#### 1. United Kingdom

Until recently, British workers, like their American compatriots, lacked substantive privacy protection. Employers could legitimately monitor and scrutinize workers' on-line activities, even when these concerned personal

---

145. *Cf.* Wilborn, *supra* note 22, at 859-60. The intrusion into one's privacy has not been shown to sufficiently impact the community as to warrant a public policy exception. *Id.* ("[C]ourts typically have prohibited recovery on this theory when purely 'private' interests are involved.... [T]hird party impacts can rarely be shown."). *But cf.* Kim, *supra* note 137, at 723 (arguing that the public policy exception protects sweeping public interest rather than third parties).

146. *See* Rothstein, *supra* note 15, at 383.

147. *Id.*

148. *See id.*

149. *See id.*

150. *See id.* (linking privacy with property and dignity with citizenship and community).

151. *Cf. id.* at 394 ("[Italian] law does not allow an individual worker to consent to . . . surveillance.").

152. *See generally id.* at 384-98.

communications. The Regulation of Investigatory Powers Act (RIPA) now provides legal redress to employees who have had their communications intercepted by an employer without lawful authority.[153] Since RIPA requires that all parties to a communication, including non-employees, consent to monitoring, employers are more likely to rely upon the ECPA-like exceptions in the regulations promulgated under RIPA.[154] It has been charged that RIPA and the regulations are not in accord with the Human Rights Act because they do not require that the invasiveness of the intrusion be proportional to the employer's legitimate need.[155]

An employer having lawful authority to intercept communications must further comply with the Data Protection Act (DPA) if personal employee information is gathered.[156] Employers who fall into the category of "data controllers" have a duty to comply with the DPA's eight "data protection principles," which are similar in tone to the PWCA proposed in the U.S.[157] Unlike employers in France, Germany, and Italy, British employers have no legal obligation to notify, much less to receive consent from, labor representatives before commencing electronic monitoring in the workplace.[158]

### 2. France

The French Labor Code requires that employers notify labor representatives or works councils of monitoring in the workplace.[159] The Labor Code also extends the provisions of the Law on Data Processing and Liberty to the workplace in the prohibition of collection of personal information on employees without notice.[160] Further, the Commission

---

153. Regulation of Investigating Powers Act, 2000, c. 23 (Eng.).

154. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, (2000) SI 2000/2699.

> Employers are permitted to monitor and intercept e-mails in order to establish facts relevant to the business; to ascertain compliance with regulatory or self-regulatory rules or guidance; to ascertain or demonstrate standards which are or should be achieved by persons using the system in the course of their duties; to prevent or to detect crime or the unauthorized use of their systems; and to ensure effective operation of the system (e.g. to detect viruses).

Gillian Morris, *English Law*, *in* ON-LINE RIGHTS FOR EMPLOYEES IN THE INFORMATION SOCIETY 125-46 (Roger Blainpain ed., Kluwer Law International 2002).

155. Morris, *supra* note 154.

156. Data Protection Act 1998, 1998, c. 29 (Eng.).

157. *Id.*

158. *See generally id.*

159. Rothstein, *supra* note 15, at 387.

160. *Id.*

Nationale de l'Informatique et des Libertes (CNIL) was created by the Law on Data Processing and Liberty.[161] To the extent that they collect data that can identify an individual, employers must file with the CNIL a description of the data collected, the legitimate purpose advanced by each use of the data, and the steps taken to ensure confidentiality.[162] As a fundamental right, privacy cannot be trampled by an employer's purely economic concerns.[163] Article 9 of the Civil Code also speaks to the notion of an individual's general right to privacy and thereby informs the analysis under similar laws.[164] Whereas French legal protections are the province of bureaucratic agencies, German law facilitates greater involvement with organized labor, and Italian privacy protection primarily rests with the unions.[165]

### 3. Germany

German privacy protection is rooted in its constitutional concept of "personality right" which is the protection of dignity against abuse of state power.[166] Employers can only legitimately interfere with an employee's right to personality if permitted by legislation, collective agreement, or if consent has been obtained from the company works council in the absence of a collective agreement on the issue. Codified protections are bifurcated, with the Telecommunications Act[167] being applicable if an employer grants employees personal use of the Internet, and the broader Data Protection Act[168] being applicable if not.[169] In general, communications monitoring by employers without employee consent is prohibited with the very rare exception of compelling interests of the undertaking or the prevention of crimes being at stake.[170] Unions, where they exist, are granted the power of "codetermination rights" on privacy issues in the workplace by the

161. *Id.* at 388.

162. *Id.*

163. Ministre du Travail v Société Peintures Corona [1980] 6 Dr. Soc. 317.

164. Rothstein, *supra* note 15, at 389.

165. *Id.* at 393.

166. GRUNDGESETZ [GG] [Constitution], art. 1 (F.R.G.).

167. des Begleitgesetzes zum Telekommunikationsgesetz (Telekommunikationsgesetz), v. 1.8.1996 (BGBl. I S.1120) (F.R.G.).

168. Deutsches Bundesdatenshcutzgesetz (German Federal Data Protection Act), v. 27.01.77 (BGBl.I S.201) (F.R.G.).

169. A. Hoeland, Use and Monitoring of E-mail in the Workplace in Germany (unpublished manuscript on file with The Bulletin of Labour Law and Industrial Relations, Kluwer Law International).

170. Landesarbeitsgericht Berlin (BAG) [Berlin Labor Court of Appeals] Der Betrieb [DB] 1024 (1988); Andrea Raffler & Peter Hellich, *Unter Welchen Voraussetzungen ist die Überwachung von Arbeitnehmer E-mails Zulässig? [Under What Conditions Is the Monitoring of Employee E-mails Permissible?]*, NZA 862, 863 (1997).

Works Constitution Act.[171] Stronger still is the power wielded by Italian labor unions, often overwhelming the right of the individual employee to consent to remote monitoring.

#### 4. Italy

In adopting the substance of the European Community Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Italy requires not only notice to the employee of data collection but also consent from the employee.[172] Stemming from an avowed purpose to protect "worker dignity,"[173] Article 4 of the Italian Workers Statute imposes an absolute prohibition on the remote monitoring of workers.[174] With respect to monitoring for productivity or safety purposes, which may have the incidental potential to monitor individuals, Article 4 requires the buy-in of works councils to permit surveillance of employees.[175] As an indication of the inalienable nature of dignity, individual employees may not consent to employer monitoring absent an agreement with the trade union.[176] Not even the "violation of employer property rights" can empower an employer to legally monitor employees.

## III. EMPLOYEE ACCESS TO E-MAIL AND THE INTERNET AT WORK

In the absence of legal recognition for electronic privacy in the workplace, the next step is to examine how a market-based solution to the issue of electronic privacy can be devised. With that objective, in this and the next sections, I first examine the underlying concerns of employers and employees regarding access to e-mail and the Internet and electronic monitoring at the workplace.

### A. *The Employer's Perspective*

Regardless of how e-mail and the Internet are used, employers invite a host of problems into the workplace when they make use of these tools.

---

171. BETRIEBSVERFASSUNGSGESETZ (Works Constitution Act), Bundesgesetzblatt [BGB1] I § 13 (1985) (F.R.G.). The Act mandates both employers and works councils to safeguard and promote the untrammeled development of the personality of employees in the establishment. *See id.* § 75(2).

172. Rothstein, *supra* note 15, at 394.

173. Gino Giugni, *Lo Statuto dei Lavoratori [Commentario of the Labor Statute]*, Giuffre', Milano (1979).

174. Rothstein, *supra* note 15, at 396.

175. *Id.* at 394.

176. *Id.*

Computer security threats, legal liability, and productivity losses may accompany the benefits of being "wired."

These days, employers have to worry about remote security breaches from the likes of school-age kids. Internet access alone makes hacking more likely.[177] Also, "[o]ne consequence of the increased use of e-mail and the Internet is that viruses are now capable of spreading many times faster than ever before."[178] Unfortunately, "[s]hort of cutting off access to the Internet, there is no such thing as absolute security in a corporate computer system."[179] While worrying about threats from without, managers should not ignore threats from within. Employees commit more computer crime against their employers than third parties do.[180] A decade ago, losses were already mounting to five billion dollars annually.[181] Employee crime is not limited to traditional white-collar embezzlement; sensitive computer information in the form of trade secrets[182] or personnel files can be altered, disclosed to others, or destroyed.[183] Unfortunately, the complete scope of computer crime perpetrated on corporations may never be known. Concerned about exposing their vulnerability to customers and to other criminals, executives are hesitant to report such crime.[184]

Of greater concern to many employers is the legal liability that may attach to a company from both the business and personal online activities of its employees.[185] Via the recent expansion of the strict liability doctrine of *respondeat superior*, an employer may be held strictly liable for the foreseeable torts and crimes of employees.[186] There is little evil under the

---

177. Stuart Rosove, *Employee Internet Use and Employer Liability*, 1997 ANDREWS EMP. LITIG. REP. 22106.

178. Diana J.P. McKenzie, *Information Technology Policies: Practical Protection in Cyberspace*, 3 STAN. J.L. BUS. & FIN. 84, 99 (1997).

179. RICHARD RAYSMAN ET AL., MULTIMEDIA LAW: FORMS & ANALYSIS § 10.08 (2001).

180. *New Hazards*, *supra* note 15, at 1899-1900 (noting that employees are more likely to commit multiple crimes over long periods of time without detection).

181. *Id.* at 1900.

182. Thomas P. Klein, *Electronic Communications in the Workplace: Legal Issues and Policies*, *in* THIRD ANNUAL INTERNET LAW INSTITUTE 720 (PLI Patents, Copyrights, Trademarks, and Literary Property Course Hand Book Series No. GO-0051, 1999). *See generally* Ari B. Good, *Trade Secrets and the New Realities of the Internet Age*, 2 MARQ. INTELL. PROP. L. REV. 51 (1998) (discussing the ease with which a trade secret can be destroyed over the Internet).

183. *New Hazards*, *supra* note 15, at 1900.

184. *Id.* at 1902.

185. *See generally* Ishman, *supra* note 4, at *19-76 (expounding upon the circumstances in which employers may be liable for employee stock manipulation, "cybersmearing," copyright and trademark violations, misappropriation of trade secrets, viruses, worms, and gambling book operations).

186. John Edward Davidson, *Reconciling the Tension Between Employer Liability and Employee Privacy*, 8 GEO. MASON U. CIV. RTS. L.J. 145, 147 (1997); *see also* Ishman, *supra* note 4, at 12-18 (demonstrating that the traditional "scope of employment" element of liability has expanded to include all acts of which an employer knows or should know).

electronic sun that cannot be accomplished without the use of e-mail or the Internet, but it is clear that mischief can be facilitated and exacerbated by these electronic tools. For example, the new electronic mediums facilitate some illegal business practices, such as the deliberate interception of competitors' secrets.[187] The ease of creating electronic communications and their irretrievable nature compound the risk of losing control of confidential information.[188] Consider the following examples in which liability may arise from a breach of computer security:

(1) A hospital that discloses confidential medical information of a patient may be liable to that patient.[189]

(2) A publicly traded company can run afoul of securities laws for leaking confidential information.[190]

Traditional torts, like defamation, may be amplified; the potential for harm through the Internet is greater due to the potential for wider dissemination.[191] Likewise, the Internet makes employee copyright infringement easier and more likely.[192] An employee may not know that the multitude of electronic documents at her fingertips is copyrighted.[193] And, since more and more software developers are turning to patent protection for their computer code, patent infringement is likely when an employee downloads a program. The proliferation of sexually graphic material on the Internet raises the specter of criminal obscenity charges, especially with regards to child pornography. The Internet further compounds the problem by largely erasing geographic and jurisdictional boundaries. It is easier to retrieve obscene material that is not considered obscene at its point of origin.[194] Vise versa, an employee may generate or send material that is not obscene where the employee sits but is so in many of the jurisdictions of the potential receivers.[195] An employer may also receive unwanted publicity when employees visit "inappropriate" Web sites.[196] "Upon

187. Rosove, *supra* note 177.

188. Rogers, *supra* note 5, at 6 ("[E]-mail is misdirected frequently enough to cause concern.").

189. McKenzie, *supra* note 178, at 94.

190. *Id.*

191. Rosove, *supra* note 177.

192. *Id.*

193. *Id.*

194. *Id.*

195. *Id.*

196. Frank C. Morris, Jr., *The Electronic Platform and Critical Employment Related Issues in the New Millennium*, *in* AMERICAN LAW INSTITUTE—AMERICAN BAR ASSOCIATION CONTINUING LEGAL EDUCATION, ALI-ABA COURSE OF STUDY: CURRENT DEVELOPMENTS IN EMPLOYMENT LAW

entering the site, the employee's 'domain name' often illustrates the name of the employer, which may be captured."[197] Given the challenges to federal electronic "decency" acts, offensive material is more likely to be the source of a claim of discrimination by contributing to the formation of a hostile work environment.[198]

The nature of electronic tools may facilitate offensive behavior and certainly increases the life span of offensive written material.[199]

> E-mail use has exploded, primarily because it is fast and easy to use. . . . These attributes also may [be] some of e-mail's biggest shortcomings. [Since e-mail is seen to be] less formal[,] . . . senders have devoted less attention to what is being written. More personal means that senders may include confidential, offensive or sensitive information, believing that they are sending private, intimate message[s] for the recipients' eyes only.[200]

An employee may write things in an e-mail that would never be written in an internal memo.[201] Or, an employee may send the e-mail to an unintended recipient.[202] Or, the intended recipient may pass it along to an audience never intended by the author.[203] With regard to "surfing" the Web, an employee's visits to offensive sites may "result in a lawsuit or appear as evidence in a lawsuit."[204] The permanence of electronic documents, and employees' ignorance of that permanence, is also troubling to employers.

> [U]nlike paper documents that can be shredded, computer files can survive long after they have been "deleted" from the system. The data remains undisturbed until more space is needed on the hard drive and then the file may be overwritten. No user can predict when, or if, a deleted file will be overwritten. Destroying an e-mail message is particularly difficult due to the fact that numerous copies may exist.[205]

---

1071, 1074 (July 27, 2000).

197. *Id.; see also* Rogers, *supra* note 5, at 5 (calling the records left behind, "cookies" or "mouse droppings").

198. Rosove, *supra* note 177.

199. *Id.*

200. Adams et al., *supra* note 101, at 33.

201. Rosove, *supra* note 177.

202. *See* Rogers, *supra* note 5, at 6 ("[E]-mail is misdirected frequently enough to cause concern.").

203. *See id.*

204. Morris, *supra* note 196, at 1073.

205. Brown, *supra* note 77, at 661-62.

Employers must worry about all these "time bombs" lurking in their computer networks because e-mail communications are legally discoverable.[206]

More pervasive than legal liability is the loss of productivity from personal use of e-mail and the Internet. Personal use does not have to be mischievous to cause harm. Time spent on personal business is time not spent working. "This is a new spin on the old nuisance of employees making personal phone calls at work, but with greatly magnified possibilities. . . . [T]he Web can be extremely seductive, lulling users to click screen after screen for hours at a time."[207] "According to one poll, almost one-fourth of an employee's time spent on-line is on nonwork-related activities."[208] Further studies show that employees "with on-line access spend up to 10 hours per week sending personal e-mail or visiting Internet sites unrelated to work."[209] Unproductive employees are the source of a litany of negative results: poor customer service, lost business, unnecessary overstaffing, high overheads, and lost profits.[210] In addition to hurting productivity, unnecessary broadcasts of personal e-mail to wide distribution lists also keep employee attention from urgent business e-mails.[211] Even when electronic tools are being used for business purposes, "[e]mployees often face 'e-mail overload' brought on by the overuse and abuse of the 'forwarding' and 'courtesy copying' features of the e-mail system."[212]

Another direct hit to the bottom line is the investment required to relieve the pressure that personal use puts on a company's scarce transmission bandwidth.[213] Large amounts of traffic are generated by inappropriate personal use and can slow network response.[214] For example, "employees often use their business Internet connection to download slow-transferring, data-heavy files, rather than using their home Internet connection."[215] Slower response means wasted time and may require an expensive network upgrade.[216] Another apparently innocuous personal use is employees shopping online at work. However, "excessive junk e-mail

206. Baum, *supra* note 20, at 1014-15.

207. Michael J. McCarthy, *Virtual Morality: A New Workplace Quandry*, WALL ST. J., Oct. 21, 1999, at B1.

208. Morris, *supra* note 196, at 1071.

209. Rogers, *supra* note 5, at 20.

210. Morris, *supra* note 196, at 1071.

211. Klein, *supra* note 182, at 715.

212. McKenzie, *supra* note 178, at 98.

213. Morris, *supra* note 196, at 1072-73.

214. *Id.*

215. Klein, *supra* note 182, at 714.

216. Morris, *supra* note 196, at 1072-73.

created by online shopping could clog a company's server and cause it to crash."[217]

It is evident that a rational employer will take affirmative steps to eliminate the risks inherent in being "wired." Eliminating liability by eliminating all employee access to the Internet and e-mail is not an economically attractive alternative. A company might as well throw all its computers in a dumpster. Employers could electronically or procedurally protect themselves in various ways. One mild example, among many, is Smith Barney, which is looking at ways to block access to hate sites.[218] A much more extreme solution is to prohibit all personal use of e-mail and the Internet in the workplace. And one may ask, why not? After all, are not the networks, the computers, and, as some would argue, the employees' time at work all owned by the employer?

### B. *The Employee's Perspective*

If only the downside of allowing employees personal use of e-mail and the Internet were considered, most employers would certainly balk. However, there are a number of practical justifications for granting some degree of access to electronic workplace tools for "appropriate" personal activities. For one, use of e-mail and the Internet enhances an employee's computer skills, which are then applied to work.[219] Accordingly, some companies believe that personal use leads to a net increase in productivity.[220] Productivity is also affected by intangible variables, such as employee morale. "[S]ome incidental personal use of the Internet is likely to improve employee morale . . . and cement employee loyalty."[221] Perhaps the reverse situation is easier to visualize. "Blocking Net access has a negative effect on employee morale . . . as employees are likely to feel they are being treated as children."[222] Worse yet prohibiting personal use can seem extremely arbitrary and can seriously harm morale in personal emergency situations.[223] Imagine a concerned parent who is prohibited from checking on a sick child by a draconian company policy.

---

217. Adams et al., *supra* note 101, at 34.

218. Rosove, *supra* note 177.

219. *Id.*

220. *Id.*

221. Michael J. Morse & Charles P. Magyera, *Internet Use Policies*, GP SOLO & SMALL FIRM L., Apr./May 1999, at 53.

222. Sindy J. Policy, *The Employer as Monitor: Keeping an Eye on Net Use and E-mails Can Prevent Litigation*, BUS. L. TODAY, Nov./Dec. 2000, at 11.

223. Lawrence A. Michaels & Lee Anne Steinberg, *Employer Monitoring of E-Mail, Voice Mail, Computer Records, and Other Electronic Information Systems—A Practical Approach*, *in* DRAFTING EMPLOYMENT DOCUMENTS IN MASSACHUSETTS § 10.11.1(d) (Mass. Continuing Legal Education ed., Supp. 1998).

> Though it might seem proper to deny use of a company's system for the employee's personal affairs, as a practical matter, it is virtually impossible for an employee to avoid using message systems for some nonbusiness matters, such as communications with family or friends on an important matter or the arrangement of social engagements with other employees.[224]

So, it is counterproductive to "criminalize" such activities, and indeed, "it is unrealistic for a company, particularly a large company, to expect all employees to refrain from any personal use of communications systems."[225]

In addition, it may also be unnecessary for a company to concern itself with the potential effect of personal use on productivity, particularly when the employee is salaried.

> [A company wants] to cut off excessive time on the Internet for hourly employees because if they are spending three hours daily on the Internet, they might be working overtime for three hours at time-and-a-half to get their jobs done. . . . But salaried employees are supposed to get their work done regardless. So as long as [salaried employees] get their work done, it is not a problem. . . . A company shouldn't care whether employees spend one or 10 hours on the Internet as long as they are getting their jobs done—and provided that they are not accessing inappropriate sites or harassing others. It is probably better that the employer stay away from the issue. Otherwise, it might lose an incredibly productive employee.[226]

Further practical considerations have led most companies to allow *some* personal activity. A company policy only controls employees; employers with e-mail systems cannot prohibit non-employees from sending personal e-mails to its employees.[227] Certainly, companies may implement technological measures to filter e-mail or to block access to certain Web sites; however, "blocking may also inadvertently prevent employees from checking legitimate, work-related Web sites."[228] The challenge of discerning what material is good from what material is bad extends to the

---

224. Trubow, *supra* note 78, at 41-42.

225. Rogers, *supra* note 5, at 20.

226. Michael A. Verespej, *Inappropriate Internet Surfing*, INDUSTRY WK., Feb. 7, 2000, at 58, *available at* 2000 WL 10594758.

227. Michaels & Steinberg, *supra* note 223, at 10.11.1(d).

228. Policy, *supra* note 222, at 11.

traditional management function of supervising employee activities. In the information age, employers can no longer monitor operations by looking over the shoulders of line workers.[229] Consequently, without some form of electronic monitoring, "it can be extremely difficult to distinguish between the employee who is busy working at his computer and the employee who is busy searching the Internet for the latest sports scores, weather reports, or worse, sexually explicit materials."[230] Thus, the same characteristic of the electronic workplace that necessitates that employees be given access to the Internet also requires that a company exert some new measure of control. But, electronic monitoring by employers disturbs the delicate balance between an employer's right to conduct business and an employee's right to privacy.

## IV. ELECTRONIC MONITORING IN THE WORKPLACE

The modern, wired workplace is an interesting forum for privacy analysis. "Two competing interests exist in the employment context: the employer's right to conduct business in a self-determined manner is matched against the employee's privacy interests or the right to be let alone."[231]

### A. *Employer's Arguments for Electronic Monitoring*

Monitoring employees is not new. Society has long recognized the practical necessity of allowing employers to supervise their employees. Employers monitor employees to get a fair day's work[232] and to protect company assets.[233] In the Nineteenth Century, Frederick Taylor built an entire discipline, Scientific Management, around monitoring.[234] The main difference between the monitoring of the past and that of today is the form it takes; in years past a person would look over the shoulder of an employee[235] while modern employers have the assistance of computers. On the other hand, once computer technology is made available in the workplace, it is a double-edged sword. Technology can be used, perhaps in unauthorized ways, by employees to check up on their superior's e-correspondence and other activities. For instance, in a recent episode in the

229. Hash & Ibrahim, *supra* note 3, at 896-97.

230. Klein, *supra* note 182, at 714.

231. Baum, *supra* note 20, at 1012.

232. Lee, *supra* note 15, at 145.

233. Hash & Ibrahim, *supra* note 3, at 897 ("[W]hat takes place on company premises, over company phones and company E-mail networks, belongs to the company which has the right to access that work product.").

234. *See* Boehmer, *supra* note 2, at 766.

235. Lee, *supra* note 15, at 143.

United States, some employees hacked into their superior's computer and discovered communications among senior management in the company discussing the imminent shutdown of a factory, even though the employees were told that no shutdown was forthcoming.[236]

While technology may hurt productivity and generate liability at one end of the equation, it may also provide the solution through cutting edge monitoring.[237] Electronic monitoring allows employers to make significant gains in the areas of productivity, quality, and safety. Monitoring enhances productivity by facilitating more efficient resource scheduling, more immediate feedback,[238] and more meaningful evaluations.[239] Quality likewise is improved, and customers benefit from better service and lower prices.[240] Monitoring is key to some safety initiatives,[241] and better safety means lower insurance premiums and workers' compensation pay-outs.[242] Payroll and equipment costs can also be reduced by monitoring employees for personal use of company equipment and for taking excessive breaks.[243] It has been estimated that employees wasted 170 billion dollars of employer time in one year alone.[244] Further savings may be realized by curbing theft and legal liability.[245]

In one year, it is estimated that employees stole the equivalent of 370 billion dollars from their employers.[246] Monitoring can be used to detect illegal or wrongful deeds so that the offenders may be punished. For example, the data flow in and out of a company can be watched to find employees transmitting sensitive data or hackers attempting to crack into the system.[247] E-mail within the workplace also can be monitored to detect

---

236. See *infra* notes 288-89.

237.

> The productivity lost and the increasing efforts of the plaintiffs' bar to sue employers based upon allegations of employee misconduct . . . [has greatly increased the need for monitoring] the conduct of employees and life in the workplace. . . . [I]t is not unreasonable to expect employers to use any and all available technologies to monitor employees' conduct.

Adams et al., *supra* note 101, at 35.

238. Shefali N. Baxi & Alisa A. Nickel, *Big Brother or Better Business: Striking a Balance in the Workplace*, 4 KAN. J.L. & PUB. POL'Y 137, 139 (1994).

239. Boehmer, *supra* note 2, at 745.

240. Baxi & Nickel, *supra* note 238, at 139.

241. *See* Flanagan, *supra* note 85, at 1262.

242. Boehmer, *supra* note 2, at 747.

243. *Id.* at 746.

244. Flanagan, *supra* note 85, at 1261 n.33.

245. *Id.* at 1261.

246. *Id.*

247. Baxi & Nickel, *supra* note 238, at 140.

electronic harassment.[248] Alternately, monitoring may be used proactively to minimize *respondeat superior* liability to detect a problem before it happens.[249] As a final incentive, the law sometimes requires employers to monitor employees.[250]

Employers do not have to monitor electronically, but they overwhelmingly choose electronic monitoring for a number of compelling reasons. First, it is often the lowest cost alternative, certainly lower than human supervisors doing the same task.[251] It is also accurate as only a computer could be, and, in the main, it is free of human biases.[252] Finally, the social landscape is primed for it. The economy has shifted from manual manufacturing to automated service industries,[253] like data processing, which is tailor-made for electronic monitoring. Union influence is declining, and along with it, a major opponent of electronic monitoring.[254] Most importantly, the employment-at-will doctrine allows employers to make employee submission to electronic monitoring as a condition of continued employment, and counter-balancing legal limitations are almost non-existent.[255]

### B. *Employee's Arguments Against Electronic Monitoring*

Employees are concerned about the effects of monitoring, and employers should take note of the consequential effects on the workplace. An employee may suffer loss of self-esteem if she interprets the monitoring to indicate a lack of trust in her.[256] Employees may also question the fairness of the monitoring: are the right variables being measured; are the wrong variables being measured; is the measurement accurate?[257] Fairness is also suspect considering that women and minorities receive a disproportionate amount of monitoring, as they make up a large percentage of the clerical ranks.[258] Worse, monitoring may be abused by the employer to intimidate and punish employees rather than help them

248. Kopp, *supra* note 36, at 864.

249. When employees build symbolic walls around themselves in an attempt to gain privacy in the workplace, sometimes employers must employ monitoring tactics which crack the employees' shell of concealment to detect future problems for which the company may be liable. *See* Davidson, *supra* note 186, at 147-48.

250. Baxi & Nickel, *supra* note 238, at 140 (citing Federal Sentencing Guidelines and FTC consent decrees as two sources of legal mandates to monitor).

251. *See id.* at 139; *see also* Boehmer, *supra* note 2, at 765.

252. Flanagan, *supra* note 85, at 1260.

253. Boehmer, *supra* note 2, at 763.

254. *Id.*

255. *Id.*

256. Flanagan, *supra* note 85, at 1264.

257. Boehmer, *supra* note 2, at 771-72.

258. Baxi & Nickel, *supra* note 238, at 140.

improve.[259] Abuse may also take the form of voyeurism,[260] union-busting, ferreting out whistleblowers, and creating pretenses to fire members of protected employee groups.[261]

The accumulation of the above effects "takes its toll on workers and companies in terms of stress, fatigue, apprehension, motivation, morale, and trust; this results in increased absenteeism, turnover, poorer management, and lower productivity, not to mention higher health-care costs."[262] Thus, monitoring may spoil the workplace environment, and it can have a detrimental effect on productivity.[263] Productivity is harmed by the mental and physical manifestations of stress: depression and anxiety,[264] including "wrist, arm, shoulder, neck, and back problems."[265] It is estimated that employee stress costs employers fifty to seventy-five billion dollars annually.[266] Monitoring can also encourage employees to act in a counterproductive manner[267] in an attempt to "game"[268] the system. Alternatively, employees may decide to avoid the use of e-mail altogether.[269] Some employees are concerned that electronic monitoring will allow employers to increase the pace of work, creating sweatshops, not unlike those before the advent of progressive labor laws.[270] Unconditional acceptance of electronic monitoring also threatens the future of privacy in the workplace. "[E]mployees, unions and advocacy groups . . . fear that without some restrictions on an employer's ability to monitor e-mail, privacy protection will all but disappear from the workplace, resulting in an 'electronic sweatshop' where constant monitoring takes place."[271]

In their path-breaking article on the right to privacy published in 1890, Samuel Warren and Louis Brandeis presaged the effect that technology would have on privacy in the workplace: "Recent inventions and business

259. *Id.* at 141.

260. Lee, *supra* note 15, at 144.

261. Boehmer, *supra* note 2, at 743.

262. Lee, *supra* note 15, at 144.

263. Baxi & Nickel, *supra* note 238, at 142.

264. Flanagan, *supra* note 85, at 1263.

265. Baxi & Nickel, *supra* note 238, at 141.

266. Flanagan, *supra* note 85, at 1264.

267. *Id.* at 1275-78.

268. Boehmer, *supra* note 2, at 772.

269. *Cf.* Natt Gantt, *supra* note 23, at 422 (predicting that, short of not using e-mail, employees might not be as candid, thus increasing miscommunication).

270. Boehmer, *supra* note 2, at 808 ("Secret monitoring is the merciless electronic whip that drives the fast pace of today's workplace in the service industry. In essence, concealed surveillance combines the worst features of 19th century factory labor relations with 20th century technology, creating an electronic sweatshop." (quoting COMM. WORKERS OF AM., Legis. Fact Sheet No. 101-2-2, *Secret Monitoring* 1-2 (1990))).

271. Adams et al., *supra* note 101, at 34.

methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual . . . the right 'to be let alone.'"[272] Though electronic monitoring is relatively new, workplace privacy disputes are not. Over the years, a certain right to privacy in the workplace has been carved out for employees in physical, personal mail and in lockers and desks. The similarity between e-mail and computer file cabinets has many commentators calling for equivalent privacy rights in e-mail.[273]

Some of the inherent characteristics of e-mail and computer storage give the appearance of traditional mail and physical storage. As with traditional mail, e-mail appears to be a private mode of communication; the recipients are chosen by the author, and there is no indication of "default" recipients. Thus, an employee may expect privacy for e-mail that is intended to be private.[274] This is the case with traditional mail. In *Vernars v. Young*,[275] the court stated that "private individuals . . . have a reasonable expectation that their personal mail will not be opened and read by unauthorized persons;"[276] so, an employer may not open an employee's personal mail.[277]

Also, the security measures applied to workplace computers and networks may also give the impression that computers are like personal desks or lockers. The holding in *K-Mart v. Trotti*[278] represents the general rule that "[e]mployees generally have a right to privacy in items locked in a desk, file cabinet, or locker if their employer does not require them to provide their supervisor with a duplicate copy of the key or combination necessary to open the lock."[279] "The use of confidential passwords and not readily identifiable user names may lead employees to believe that their e-mail and internet postings are confidential or anonymous, and that they have a right to privacy in such electronic communications."[280] "Courts could easily view mailserver's memory as a locker or file cabinet and the password as a lock."[281] This point of view, however, is not pervasive. Thus, employees have a vested interest in how courts interpret the law of the land as applied to e-mail.

---

272. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

273. Lee, *supra* note 15, at 144.

274. Schnaitman, *supra* note 29, at 202-03.

275. 539 F.2d 966 (3d Cir. 1976).

276. *Id.* at 969.

277. Beeson, *supra* note 42, at 213.

278. 677 S.W.2d 632 (Tex. Ct. App. 1984).

279. Beeson, *supra* note 42, at 214-15.

280. Brown, *supra* note 77, at 647.

281. Beeson, *supra* note 42, at 214.

## V. GUIDING PRINCIPLES IN FASHIONING A SOLUTION

As we have seen earlier, in the U.S., neither statutory law nor the common law recognizes a zone of privacy in the workplace. Some progressive academics, such as Anita Allen, urge that an emphasis on creating a zone of privacy in the workplace works against the interests of women seeking to be free from sexual harassment and gender-related misconduct in the workplace.[282] Further, unlike in some European countries, in the United States, no universal right to privacy or human dignity has been established, and therefore, the government lacks a fundamental instrument to fashion a privacy zone at work. In the future, perhaps Congress or the courts will step in and vindicate privacy interests in the workplace. When federal appellate and district court judges, including Judge Alex Kozinski and Judge James Rosenbaum, discovered that all their online activity was being monitored by the Administrative Office of the Courts, an angry response followed, and a subsequent review of court system administrative procedures was sought. This provides hope that, in the future, courts might step in to limit employer monitoring of their computer networks.[283] But, given our past record in this area, that possibility is remote. However, legal remedies are not the only option. The market has a role to play in crafting a solution that addresses the differing, and perhaps conflicting, interests at work.

In this section, I propose a contractarian solution to the problem of electronic privacy in the workplace that maximizes the interests (i.e., the payoffs) of both employers and employees. Relying on insights from microeconomic, principal-agent models, I show that it is possible to define an e-policy contract for the workplace that is compatible with the incentives of employees and employers by incorporating the following principles into the contract: (a) participation by employers and employees in jointly defining workplace e-policies, and employee commitment to adhere to these commonly-defined e-policies; (b) full disclosure by

282. Anita L. Allen, *The Wanted Gaze: Accountability for Interpersonal Conduct at Work*, 89 GEO. L.J. 2013, 2027 (2001) (advising that women must cooperate with employers and permit responsible, privacy-sensitive monitoring at work).

283. *See* Ted Bridis & Glenn R. Simpson, *Judges' Ire Stirs Debate on Web Monitoring*, WALL ST. J., Aug. 9, 2001, at B9 (noting that a dispute within the federal judiciary over Internet use provides hope that federal laws on employee monitoring of company computer networks might change); Neil A. Lewis, *Rebels in Black Robes at Surveillance of Computers*, N.Y. TIMES, Aug. 8, 2001, at A1 (noting that Chief Judge Mary Schroeder of the Ninth Circuit was "concerned about the propriety and even the legality of monitoring Internet usage"); Carl S. Kaplan, *Reconsidering the Privacy of Office Computers*, N.Y. TIMES (July 27, 2001), at http://www.nytimes.com/2001/07/27/ techn (stating that Judge James M. Rosenbaum, Chief Judge of the U.S. District Court for the District of Minnesota, expressed uneasiness over the proposition that employers may freely rummage through employee computers at work).

employers of implementation measures, in accordance with these e-policies; and (c) implementation measures to include monitoring of employers to ensure compliance with e-policies. As discussed below, I show that such a contract maximizes the benefits and reduces the losses that accrue to both employers and employees.

### A. *Applying Principal-Agent Theory to Electronic Privacy in the Workplace*

The Internet at the workplace helps workers improve their productivity, especially in those activities related to information gathering or processing. It is also useful to those businesses embarking on online commercialization of their products. In these cases, the existence of the Internet is key to the normal development of their business activities. But, workers can access the Internet, not only for work-related tasks, but also for personal reasons. The latter use could diminish workplace productivity.[284] Thus, it is an objective of the employer to: (a) reasonably limit personal use of the Internet by employees; (b) forbid certain other uses of the Internet, such as seeking adult entertainment or harassing fellow employees; and (c) encourage Internet use for work-related activities.

The situation described above can be related to the familiar principal-agent problem in microeconomic theory.[285] Here, the employer is the principal and the employee is the agent. In this model, the principal expects some level of effort by the agent in order to attain a desired level of output. For the agent, work impacts his utility function negatively, and so he will try to cheat on the principal and supply a lower level of effort. It is in the agent's interest to supply the least amount of work to attain the expected level of output, assuming that this output can be verified by the principal. In short, the agent is assumed to be work-averse and risk-averse.[286] The agent also has private information, for example, knowledge about computer systems at work, that the principal cannot get access to without incurring some cost, i.e., paying some compensation or rent to the agent for such information. The problem of the principal is that she cannot observe the amount of work-related effort that the agent expends, except through other signals. These signals are not necessarily related to the agent's true level of effort, and it could even be misleading. The optimal solution to this problem is for the principal to offer a contract that is compatible with

284. *See supra* notes 207-10 and accompanying text.

285. For a good introduction to principal-agent models, including problems and criticisms of this approach, see Stanley Baiman, *Agency Research in Managerial Accounting: A Second Look*, 15 ACCOUNTING ORG. & SOC. 341, 342-46 (1990) or Andrei Shliefer & Robert W. Vishny, *A Survey of Corporate Governance*, 52 J. OF FINANCE 737, 740-48 (1997).

286. Baiman, *supra* note 285, at 343.

both the agent's and her own incentives. Such an optimal contract would leave the agent indifferent, or better off, between supplying the right amount of effort and not doing so. In principal-agent theory, a fully cooperative solution is not attained because both parties are motivated by their own self-interests. Instead, the goal is to formulate an optimal contract that provides an incentive-compatible solution, thereby maximizing the payoffs to both principal and agent. Finally, the principal can monitor or control the agent's activities and penalize the agent in case of no compliance with the required effort or desired output.

These principal-agent models and their optimal solutions are easy to implement in traditional work environments, but they turn out to be more complex with the Internet due to the following characteristics.

First, easy access to the Internet makes it quite difficult for the principal to supervise and control the activities of the agent.[287] For example, it is more difficult for the employer to control Internet activities and monitor for excessive or forbidden Internet use compared to the use of an office phone. While the principal's costs of control or monitoring may be reduced by the use of new technology and computers, this new technology is also available to the agents who may use it to avoid being detected. Thus, information technology advances are available to both parties and controls are easier to avoid.[288]

Second, computer network interconnections with the outside world makes it difficult to control incoming and outgoing flow of information both to and from the firm. As a result, confidential business information can be easily transferred to the competition using the Internet, and these violations can be hard to detect in a timely fashion.[289]

Third, the Internet opens up multiple opportunities for any person to increase her utility. Therefore, completely prohibiting Internet use can undermine worker effort and reduce productivity even more than the case when some Internet use is permitted. The new technology gives users a new world to explore and interact with and enables new and different transactions. Therefore, agents are likely to achieve higher levels of utility compared to using telephone or fax machines. As a whole, the use of the Internet increases productivity and enhances the operating efficiency of firms. This high level of utility that is derived from Internet use can also

287. *See* Michelle Conlin & Alex Salkever, *Revenge of the Downsized Nerds*, BUS. WK., July 30, 2001, at 40 (noting that companies are vulnerable to employee computer sabotage and quoting FBI estimates that each insider computer attack costs on average $2.7 million).

288. *See id.* (noting that employees are seeking revenge on former employers and companies are fighting back with their own measures).

289. *See* Edmund Tee, *More to Fear from Staff Than Hackers*, THE STRAITS TIMES, Jan. 26, 2001 (citing a U.S. Computer Security Institute and FBI survey showing that seven out of ten times, a company's intellectual property is stolen by its employees).

make agent compensation and control too expensive, or prohibitive, for some firms.

Fourth, use of the Internet expands workplace productivity, but normal standards for performance have yet to be developed. Since the Internet is still growing and multiple uses are being created all the time, it is difficult to establish some parameter for productivity. Most of the existing productivity parameters are obtained from tasks done under traditional technologies. Thus, it is difficult to measure the effort at work through signals that the agent sends to the principal. This increases the probability of cheating by the agent and also increases the probability of error in the principal's evaluation of the agent's efforts.

Fifth, the use of the Internet can take power away from managers and distribute it to the workers. This result is derived from all the factors mentioned above. In addition, the decentralized and non-geographic characteristics of the Internet make it difficult for an entity to centrally control its operations, thereby further reducing the power of the principal.

In sum, the introduction of the Internet into the workplace has the following effects:[290]

- Difficulty in establishing control over the activities of the agent
- Difficulty in controlling flow of information to and from the firm
- Higher levels of efficiency and utility derived from Internet use in the workplace
- Difficulty in establishing productivity standards and measures to evaluate agent performance
- Loss of the principal's power and lesser ability to take effective, unilateral action.

Given the new characteristics derived from the presence of the Internet at work, there are new and greater incentives for both principal and agent to

---

290. Consideration must also be given to the limitations on choice that are imposed by the very nature of the Internet. *Cf.* Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 822-23 (2000).

> Beyond information asymmetries and the collective action problem, another limitation on the choice-making of individuals in cyberspace concerns bounded rationality. In particular, when faced with standardized terms, individuals left by privacy-control to fend for themselves will frequently accept whatever industry offers them. As scholarship in behavioral economics has demonstrated, consumers' general inertia toward default terms is a strong and pervasive limitation on free choice.

*Id.*

design an optimal contract that is compatible with both their self-interests. The Internet increases the transaction costs of establishing a contingent contract given the numerous ways that an agent can avoid employer controls, the easy access to vital information, and the higher utility derived from personal access to the Internet. It thus raises the possibility of moving away from purely self-interested behavior and reaching for a tacitly cooperative solution between the principal and agent. The transaction costs of achieving such a contractual solution between the principal and agent may be lower and more efficient in the new context.

The principal, i.e., the employer, may eliminate the negative effects from Internet use at work by not wiring the workplace, but that option is costly for the employer since she loses all the economic benefits and competitive advantages derived from using the Internet in her company. The agent may also seek higher compensation to join such a workplace. Finally, the agent may, nevertheless, be able to evade the employer's rules by accessing the Internet during work hours using palmtop or personal communicator devices with wireless Internet connections.

The agent, i.e., the employee, can create a zone of privacy by completely avoiding any personal use of the Internet at work. But this is costly to the employee since it creates significant inconvenience and may result in some monetary loss as well. Surreptitiously accessing the Internet in a draconian workplace without computer access is also not beneficial to the agent as he has to deal with the fear and uncertainty of being detected and punished for his conduct.

Consequently, it may be possible to achieve a lower-cost, economically efficient solution to the problem of electronic privacy in the workplace that is based on an incentive-compatible agreement between the parties. The guiding principles for such an optimal contract between the principal (i.e., employer) and agent (i.e., employee) that develops mutual trust are:

(a) Participation by employers and employees in jointly defining workplace e-policies, and employee commitment to adhere to these commonly-defined e-policies;
(b) Full disclosure of implementation measures, in accordance with these e-policies;[291] and
(c) Implementation measures to include monitoring of employers to ensure compliance with e-policies.

291. Although a large percentage of firms that monitor employees' online activities disclose that fact, see 2001 AMA Survey, *supra* note 9 and accompanying text, it is unclear to what extent they disclose and clarify permissible, excessive, and forbidden uses of the Internet and also reveal the details of their monitoring activities and tracking schemes.

Specifically, the agreement between the principal and the agent should contain the following: The principal recognizes that the Internet increases the agent's utility, and therefore, she must define prohibited and excessive uses of the Internet in consultation with the agent or other representatives of the agent and seek the agent's buy-in with respect to those e-policies. The details regarding Internet use in the workplace must be specified, and the agent and the principal must commit to following these e-policies. In order to avoid misuse, since the agent still has an incentive to cheat or free ride against other workers, a level of monitoring or control will be established.

This contract maximizes the expected payoffs for both principal and agent. The employer's benefits are as follows: (a) enhancing the firm's competitiveness by employing the Internet at work; (b) controlling the agent's use of his superior information through monitoring for compliance; and (c) permitting enforcement of e-policies by putting the agent on notice and by obtaining the agent's buy-in and commitment to these e-policies. The employee's benefits are as follows: (a) participating in fashioning e-policies, thereby ensuring that his point of view is heard and accommodated; (b) enhancing his utility through some personal Internet use at work; and (c) avoiding a workplace environment governed by fear, uncertainty, and doubt (i.e., a FUD regime). The employer would rather not have to suffer some economic loss arising from employees' personal Internet use, and the employee would rather not be subject to electronic monitoring at work. But these losses are far outweighed by the benefits arising from the incentive-compatible, contractual solution outlined above.

Furthermore, by defining such a contract informed by these principles, the agents know what the company expects from them, and they also know that they can use the Internet for specific, non-work related purposes. Therefore, it is optimal for them to offer the requisite quantity of effort in order to avoid being caught, fired, or sanctioned and to adhere to the rules governing non-work related Internet use. Since some personal use is permitted, employees have no incentive to expend resources in masking personal activities, and therefore, control or monitoring costs accrued by the principal are expected to decrease. Indeed, employees may penalize each other for bad behavior or for deviations from the norm. Since high levels of deviation from the set standards or cheating can result in a stricter regime or a return to a less desirable scheme, employees can collude in order to denounce or penalize those who deviate from the agreement.[292]

---

292. This result is attainable as long as the agreement makes everybody better off than a strictly non-cooperative, principal-agent contract. This is especially true if the expected utility from cheating today and then being penalized later is lower than not cheating at all. If enough employees are in such a situation, then their collective agreement could turn down individual behavior, and they could collude to avoid deviations.

The interaction between employers and employees can help to define some gray areas like productivity requirements and the firm's objectives. In general, the workers have better information regarding the capabilities and their use of the Internet, and the firm also knows and understands its objectives and requirements better. Both parties can then find an optimal arrangement in order to define the optimal level of employee effort needed to reach a desired productivity level in exchange for time to use the Internet for personal activities. This type of incentive-compatible contract based on full disclosure, employee participation in defining e-policy, and employer monitoring can promote mutual trust[293] and embody the firm's commitment to fair dealing.[294] This approach can, in turn, produce more economically efficient results compared to other agreements based largely on self-interested behavior by the principal. This solution is also consistent with other recent work by Cooter and Eisenberg showing that agents can internalize fairness norms that are firm-specific and engage in more cooperative behavior thereby creating value and contributing to profits.[295]

Relying on the employer and employee to contractually seek a solution is made even more appealing when the subject matter is electronic privacy. In cyberspace "bottom-up" regulation, like the approach advocated here, can be superior to "top-down" regulation, like federal statutes.[296] In the dynamic environment of computing, statutes may be more uniform and inflexible than the situation requires.[297] New problems in cyberspace are particularly suited to the lowest level of control. Therefore, a contractual solution can provide a better solution, especially in the absence of externalities.[298] With respect to e-mail privacy in the workplace, since

---

293. Winters, *supra* note 27, at 105-06 (noting that "[i]mplicit within the employer-employee relationship is some element of trust. Trust engenders teamwork, and teamwork sets the stage for increased productivity").

294. Flanagan, *supra* note 85, at 1280-81 ("Implementing an articulate workplace electronic privacy policy . . . would greatly reduce the adversarial relationship between employers and employees that is often a product of secretive monitoring, thereby fostering a more cooperative relationship. Such cooperative relationships would produce a 'win-win' situation. Employees would benefit from an improved working environment, and employers would profit from increased productivity. Realizing the opportunity to create this mutually advantageous situation, some companies already have entered into discussions with employees to create an internal electronic privacy policy closely resembling the Act.").

295. *See* Robert Cooter & Melvin A. Eisenberg, *Fairness, Character and Efficiency in Firms*, 149 U. PA. L. REV. 1717, 1717 (2001) (urging that firm-specific, fairness-specific norms can be internalized by agents and promote efficiency).

296. Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993, 1025 (1994); Jay P. Kesan & Andres A. Gallo, *Neither Bottom-Up Nor Top-Down: A Tacit Public-Private Cooperative Solution for Internet Regulation* (forthcoming in 2002), available on Social Science Research Network, *at* http://www.ssrn.com.

297. Hardy, *supra* note 296, at 1025.

298. *Id.*

employer and employee are already in a working relationship, the transaction costs for implementing the approach described above will be low.[299] Furthermore, companies vary widely as to how much e-mail security they require, and employees can also vary as to how much electronic privacy they demand.[300] Taking into account how "hard [it is] to know what 'e-mail in the workplace' will look like in only a few years' time" indicates how unsuitable a uniform, universal, statutory solution might be.[301] Even commentators who are skeptical about law and economics insights with respect to electronic privacy still conclude that a market solution is superior to government regulation in this arena for two reasons: (1) "ease" of evasion would make enforcement difficult, and (2) the variation across all companies eliminates the possibility of a fair, yet uncomplicated, law.[302]

It is possible that we might see a legislative response to the concerns of employees and employers regarding e-mail and Internet use and workplace monitoring. Such a legislative solution can incorporate the contractarian proposal outlined above by codifying the principles of employee participation in creating e-policy, complete disclosure of implementation measures, and support for employer monitoring. In the past Congress has attempted to pass statutes requiring notice of electronic monitoring.[303] These attempts, however, have included a near-universal ban on continuous monitoring, and hence, they were not successful due to opposition from the business world.[304] The proposal outlined in this Article attempts to find a solution that is compatible with the incentives of employees and employers and is therefore more likely to be embraced by both camps during the legislative give-and-take.

Finally, in order to devise a practical system for independent employee participation in developing e-policies, in some workplaces, it will be necessary to ensure that there is no employer domination or control,[305] in accordance with Section 8(a)(2) of the National Labor Relations Act (NLRA).[306] This may require the formation of a "privacy committee" or

299. *Id.* at 1032.

300. *Id.*

301. *Id.* at 1033; Kesan & Gallo, *supra* note 296.

302. Davidson, *supra* note 186, at 166.

303. *See supra* note 80 and accompanying text discussing the PWCA.

304. *See supra* notes 80-89 and accompanying text.

305. I am grateful to my colleague, Matt Finkin, for bringing this issue to my attention and for educating me about Section 8(a)(2) of the NLRA. *See* Matthew W. Finkin, *Bridging the "Representation Gap,"* 3 U. PA. J. LAB. & EMP. L. 391, 413 (2001) (urging formation of independent, employee-elected committees to bridge the representation gap and outlining how these committees might be established without running afoul of section 8(a)(2) of the NLRA).

306. 29 U.S.C. § 158(a)(2) (2001) (corresponding to section 8(a)(2) of the NLRA that outlines unfair labor practices).

"information technology committee" with elected representatives who are given the responsibility of dealing with management in formulating rules and policies. A detailed discussion of the compatibility *vel non* between Section 8(a)(2) of the NLRA and implementation of this proposal is beyond the scope of this Article.

In the next section, I will discuss the specific content of e-policies implemented within the framework outlined above.

### B. *Defining Workplace E-Policies*

Workplace e-policies must articulate clear standards to minimize employment disputes and must enable consistent administration of employer-employee relations.[307] Recognizing that a carefully crafted computer and Internet use policy must incorporate significant details regarding permissible, excessive, and forbidden use, in this section, I will highlight the key areas that ought to be considered. The specific policy features selected depend on the specifics of an individual workplace, but most policies must contain some common elements.[308]

The typical areas that ought to be addressed are:[309]

(A) Establishing ownership and user guidelines for computer and Internet use: for example, considering outlining appropriate business use and personal use of computers and the Internet, specifying forbidden content and forbidden use, and specifying the employer's right to access e-mail on the employer's computer system.

(B) Defining monitoring policies and procedures and informing employees about the details of such monitoring (see next section).[310]

---

307. Baum, *supra* note 20, at 1035.

308. Brown, *supra* note 77, at 670.

309. Some examples of policies may be found in the following sources: Brown, *supra* note 77, at 670-73; RICHARD RAYSMAN ET AL., MULTIMEDIA LAW: FORMS AND ANALYSIS § 10.08 (2000) (giving policies specifically directed to e-mail, offensive communications, trade secrets, and unsolicited ideas, online copyright infringement); *Setting up a Corporate Policy for Internet Use: A Checklist*, COMPUTER L. STRATEGIST, Oct. 1995, at 4; Klein, *supra* note 182, at 749-54; Erik J. Blanoff et al., *E-mail: Property Rights vs. Privacy Rights in the Workplace (with Model Consent Forms and Communications Policy)*, 45 No. 8 PRAC. LAW. 29, 50-53 (Dec. 1999); and Arthur D. Rutkowski & Barbara Lang Rutkowski, *Update on E-mail (Computer, E-Mail, Voice Mail and Internet Access)*, 15 NO. 9 EMP. L. UPDATE 3 (Sept. 2000).

310. Michaels & Steinberg, *supra* note 223, at 10.11.1(a).

(C) Educating employees about the risks of using e-mail and the Internet.[311] For example, consider informing employees:

- that e-mail is irretrievable.
- that Internet activities can be traced by third parties.
- about download procedures and the risk of viruses.
- about prohibitions on inappropriate and illegal uses.

(D) Limiting employer liability: for example, include information designed to curtail employee conduct for which the firm may be liable.

- Harassment, discrimination and defamation claims.[312]
- Copyright and patent infringement issues,[313] specifying limits on what might be downloaded from the Internet or exchanged through e-mail.
- Revealing confidential information.
- Informing employees of circumstances that may lead to liability.[314]
- Using technological means to prevent trade secret and confidential files from being transmitted.
- Mandating the use of encryption software or banning the transmission of sensitive information.
- Creating an approval policy for information to be published on the Web.

### C. *Monitoring*

The very existence of a monitoring program reduces employee abuses.[315] Since monitoring can have a negative impact on employee morale,[316] monitoring should be narrowly tailored to satisfy business-related, administrative, or legal needs, and any review of personal e-mail ought to be limited to ensure protection of personal information.[317] One option that has been proposed is using a third party to perform the monitoring so as not to have the employer uncover personal, but potentially appropriate, visits to web sites providing information about cancer, substance abuse, and the like.[318] In addition, there are technology measures that fall short of monitoring e-mail but are nevertheless quite

311. Morse & Magyera, *supra* note 221, at 53-54.
312. Rosove, *supra* note 177.
313. McKenzie, *supra* note 178, at 90.
314. *Id.*
315. *See* Morris, *supra* note 196, at 1099.
316. Baum, *supra* note 20, at 1041 n.153.
317. Adams et al., *supra* note 101, at 45.
318. Morris, *supra* note 196, at 1099.

effective, even if somewhat less so in terms of detecting e-mail-related non-compliance. For example, "blocklists" can be set up to deny access to offensive URLs.[319] Other programs that still fall short of monitoring e-mail may be used to monitor Internet statistics such as visits and time spent at Web sites.[320] One such product is eSniff, which "monitors all network traffic and flags activity that could cause problems. It defines categories, then analyzes the content and context of all computer network activity to determine if any communication falls into a category that an employer has established as inappropriate."[321]

## VI. CONCLUSION

It is well established that neither statutory law nor the common law in the U.S. guarantees an employee's right to privacy in the workplace. Drawing upon principal-agent theory, I show that we can address the underlying concerns of employers and employees functioning in a wired workplace in a contractarian framework. I contend that a modern, computerized workplace reduces the powers enjoyed by the principal and reduces her ability to act against the agent unilaterally and effectively. Hence, we can design an incentive-compatible, benefit-maximizing contract between employers and employees based on the following principles: employee participation in defining e-policies; full disclosure of all implementation schemes pursuant to these e-policies; and employer monitoring to ensure compliance with such e-policies. In addition, such an optimal contract promotes mutual trust and fair dealing and cultivates the formation of fairness norms, which in turn, increases productivity and contributes to higher profits. Finally, should Congress decide to act, the principles outlined above can serve as the basis for new legislation in this arena.

319. *Id.* at 1098.

320. Rosove, *supra* note 177.

321. Policy, *supra* note 222, at 11 (describing the eSniff software).