Washington University Global Studies Law Review

Volume 4 | Issue 2

January 2005

Monitoring E-mail of Employees in the Private Sector: A Comparison Between Western Europe and the United States

Yohei Suda
Supreme Court of Washington

MONITORING E-MAIL OF EMPLOYEES IN THE PRIVATE SECTOR: A COMPARISON BETWEEN WESTERN EUROPE AND THE UNITED STATES

YOHEI SUDA*

Abstract: Both Western Europe and the United States limit e-mail monitoring by an employer in the workplace and protect employee privacy. Nevertheless, cases from both Western Europe and the United States show that these regions allow an employer broad rights to monitor employee e-mail. A new case from France, however, demonstrates that Western Europe is increasingly likely to protect employee privacy in the workplace by limiting e-mail monitoring by private-sector employers. Conversely, little is expected to change in the United States, despite recent corporate scandals, because the role of government and the value placed on the right to privacy diverges in the United States from that of Western Europe.

I. INTRODUCTION

Employee communication in the workplace is increasingly under employer surveillance.[1] According to a recent survey in the United States, forty-seven percent of large and mid-sized organizations monitor employee e-mail messages, and sixty-three percent monitor their Internet use.[2] Another survey in the United Kingdom revealed that up to eighty-four percent of businesses monitor employee communication.[3]

---

* Law Clerk for the Honorable Barbara A. Madsen of the Washington State Supreme Court (2003–2004); Maîtrise (2003), Université de Nantes; J.D. (2002), University of Washington; LL.B. (1999), University of Tokyo. The author would like to thank Professors Patrick Chaumette, Christopher Docksey, Karen Williams, Walter Walsh, and Joel Reidenberg for their kind guidance and suggestions. This Article reflects only the author's personal view and in no way implicates the view of the Washington State Supreme Court.

1. Michael Osterman, *Employee E-mail Surveillance*, NETWORK WORLD FUSION, *at* http://www.nwfusion.com/newsletters/gwm/2000/1204gw1.html (last visited Nov. 16, 2004). The storage and review of employee e-mail messages has increased dramatically since 1997. According to one survey, 14.9% of organizations conducted reviews of employee e-mail messages in 1997, "while the 2000 survey reveal[ed] that 38.1% of organizations [did] so." *Id*.

2. American Management Association, *More Companies Watching Employees, American Management Association Annual Survey Reports*, *at* http://www.amanet.org/press/amanews/ems2001.htm (last visited Nov. 16, 2004) [hereinafter AMA Reports]. This survey is based on the answers of 1,627 respondents, many of whom are large companies in the United States. Thus, these results reflect the trend in large U.S. companies. According to this survey, 77.7% of employers actively monitor some form of employee communication, including voice mail and telephone conversations. *See* American Management Association, *2001 AMA Survey, Workplace Monitoring &*

In some cases, the result of such surveillance is serious. In November 1999, *The New York Times* fired twenty-three employees for allegedly distributing offensive jokes on the company's computer system.[4] Xerox fired forty employees for violations of the company's e-mail policy.[5] In fact, more than a quarter of large- and mid-sized companies have fired employees for the misuse of office e-mail and Internet services.[6]

When an employer monitors employee e-mail, there is a conflict between employer and employee interests. On the one hand, an employer has varied and legitimate interests in monitoring employee e-mail. First, they have an interest in preventing viruses and hackers from penetrating the office computers and servers.[7] An employer also has legitimate interests in preventing employees from disseminating trade secrets, sending e-mail that can provoke lawsuits, and reducing their productivity.[8]

Surveillance: Policies and Practices, Summary of Key Findings, *available at* http://www.amanet.org/research/pdfs/emsfu_short.pdf (last visited Nov. 16, 2004) [hereinafter AMA Survey].

3. Matthew Glynn, *When E-mail Must Remain Private: Data Protection: Companies Can Monitor Employees' Messages. But They Must Be Careful, Says Matthew Glynn*, FINANCIAL TIMES, June 4, 2001, at 13, *available at* 2001 WL 25827450.

4. Thomas York, *Invasion of Privacy? E-mail Monitoring Is On The Rise: Businesses Can—and DO—Monitor Messages to Avoid Legal and Technical Problems*, INFORMATION WEEK, Feb. 21, 2001, *at* http://www.informationweek.com/774/pre-mail.htm (last visited Nov. 16, 2004). *The New York Times* found the messages, which it considered obscene, through an investigation of an employee's use of company stationery to obtain unemployment benefits for a friend. *See* Lisa Guernsey, *Management: You've Got Inappropriate Mail; Monitoring of Office E-Mail Is Increasing*, *at* http://www.somansa.com/english/abou_press.htm (last visited Nov. 16, 2004).

5. Maura Kelly, *Your Boss May Be Monitoring Your E-mail*, SALON.COM, Dec. 8, 1999, *at* http://dir.salon.com/tech/feature/1999/12/08/e-mail_monitoring/index.html?sid=497303 (last visited Jan. 10, 2005).

6. "More than a quarter of surveyed companies (27%) say that they have fired employees for misuse of office e-mail or Internet connections, and nearly two-thirds (65%) report some disciplinary measure for those offenses." AMA Reports, *supra* note 2.

7. MATTHEW DANDA, LA SECURITE SUR LE WEB 16–17 (2001). This is mostly the task of a webmaster appointed by an employer. However, scholars and practitioners seem to prefer the expression "monitoring by an employer." This Article reflects this preference.

8. *See* Dana Hawkins, *Lawsuits Spur Rise in Employee Monitoring*, U.S. NEWS & WORLD REPORT, Aug. 13, 2001, at 53, *available at* 2001 WL 30365775; David Russell, *One-Third of U.S. Workers Have Web Use Monitored*, TORONTO STAR, July 11, 2001, at E05, *available at* 2001 WL 23661745. *Cf.* Press Release, Websense, Employee Internet Misuse a $63 Billion Problem for Corporate America, Reports Websense Inc.: Misuse May Affect U.S. Productivity Overall, Which Recently Hit Eight-Year Low (Aug. 1, 2001), *at* http://www.websense.com/company/news/pr/Display.php?Release=010801355 (last visited Nov. 16, 2004) (pointing out that employees' Internet use for non-work-related websites is responsible for low work productivity). The survey by the American Management Association showed that legal liability, security concerns, and productivity measurement are the top three rationales for electronic monitoring and surveillance. According to the survey, legal liability was the most important rationale, with a rating of 5.89 on a scale from one, as the lowest or least important, to seven, as the highest or most important rating. Security concerns were the second most important rationale, with a rating of 5.65, followed by productivity, with a rating of 5.06. Among those companies that brought legal actions concerning employee e-mail and Internet use, legal liability's rating increased to 6.30. *See* AMA Survey, *supra* note 2.

On the other hand, monitoring employee e-mail inevitably compromises employee privacy in the workplace. Because employees tend to send personal e-mail from work, particularly outside work hours, monitoring provides an employer with access to personal matters.

This conflict between employer and employee interests is not new. The employer who opened a letter addressed to her employee or who monitored an employee's telephone conversation raised the same issues. It is important, however, to consider the conflict in the context of e-mail monitoring because it has become significantly easier for employers to monitor employee e-mail in the workplace as enabling technology has advanced and become available at a lower cost.[9]

In 1989, the Council of Europe adopted a recommendation to further the protection of employee privacy in the workplace.[10] Additionally, on October 24, 1995, the European Union adopted Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data.[11] Directive 95/46 creates a

---

9. *See generally* S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace*, 32 GA. L. REV. 825, 826–27 (1998) ("[t]he technology allows surreptitious and continuous surveillance"); Larry O. Natt Gantt, II, *An Affront to Human Dignity: Electric Mail Monitoring in the Private-sector Workplace*, 8 HARV. J.L. & TECH. 345, 345 (1995) ("[T]he current widespread development of sophisticated technology is greatly expanding the advanced and highly effective methods by which employers monitor the workplace."). "American workers are coming under scrutiny via technology such as e-mail scanning software and satellite tracking devices." Tammy Joyner, *Atlanta-Area Employees Chafe at Employers' New Monitoring Systems*, ATLANTA JOURNAL AND CONSTITUTION, July 25, 2001, at 01, *available at* LEXIS, News Library, Atlanta Journal-Constitution File. "Such monitoring through video equipment, point of sale technologies, computer terminals, magnetic 'active' badges pen registers, telephone recording devices and numerical control machines now allows access to most, if not all, employee conversations and e-mail, and in many cases can record each movement or keystroke of an employee." Lawrence E. Rothstein, *Privacy or Dignity?: Electronic Monitoring in the Workplace*, 19 N.Y.L. SCH. J. INT'L & COMP. L. 379, 379 (2000). "Sales of employee-monitoring software are worth about $140 million a year, a return to the vendor of only a few dollars per covered employee: on average, only about $5.25 per monitored employee per year (and as little as $4 per employee, when the non-monitoring uses of these products, such as filtering for spam or viruses, are included). Even considering reseller discounts and hardware costs, a large organization may end up paying less than $10 per year per monitored employee. For example, the U.S. Army recently purchased a 200,000-seat installation from Websense; including hardware, the total cost was $1.8 million, or only about $9 per employee." Andrew Schulman, *The Extent of Systematic Monitoring of Employee E-mail and Internet Use*, SONIC.NET, July 9, 2001, *at* http://www.sonic.net/~undoc/extent.htm (last visited Nov. 16, 2004).

10. COUNCIL OF EUROPE, *Recommendation of the Comm. of Ministers to Member States on the Protection of Personal Data Used for Employment Purposes*, Recommendation No. R (89) 2 (1989), *available at* https://wcm.coe.int/ViewDoc.jsp?id=710373&Lang=en (last visited Nov. 16, 2004) [hereinafter Council of Europe Recommendation]. It is important to keep in mind that the Council of Europe and the European Union are separate bodies.

11. Council Directive 95/46/EC of 24 October 1995 on the Protection of individuals with regard to the processing of personal data and on the free movement of such data,1995 O.J. (L 281), *available at* http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=31995L0046&model=guichett (last visited Nov. 24, 2004) [hereinafter Directive 95/46].

comprehensive legal scheme designed to protect citizens' privacy against private parties.[12] However, the right to privacy protected by the Directive has some exceptions.[13] For example, case law addressing private-sector employee surveillance does not appear to favor employee privacy.

In the United States, federal legislation as well as state statutes and common law regulate employer monitoring of employee e-mail.[14] However, these laws do not sufficiently protect employee privacy, and exceptions to federal legislation undermine its protection. Moreover, a common-law action for invasion of privacy against a private party, such as an employer, is difficult to establish in state court. And actions under both state and federal statutes have problems similar to those brought under the common law.

Recent events, however, may change the landscape of this issue. On October 2, 2001, the *Cour de cassation* (Court of Cassation), France's highest court, rendered a judgment that severely restricted an employer's right to monitor their employees' e-mail. And in the United States, a series of corporate scandals raised the serious issue of an employer's ability to manage the day-to-day functioning of a corporation.

This Article demonstrates that the level of protection currently given to employee e-mail in the private-sector is similar in Western Europe and in the United States, though Western Europe appears to provide greater protection. On the other hand, this Article argues the judgment of the *Cour de cassation* in *Nikon France v. Odof* indicates that Western Europe, unlike the United States, will likely increase the level of privacy protection afforded employee e-mail.[15]

The right to privacy enjoys a higher status in Western Europe than in the United States. Additionally, while in Western Europe the government plays an active role in protecting citizens' rights, there is a traditional skepticism toward government in the United States. Thus, governments in Western Europe can more easily intervene in an issue between two private parties in order to protect employee privacy and limit e-mail monitoring by an employer. On the other hand, the U.S. government is not likely to

12. The European Commission, *Data Protection*, Jan. 10, 2005, *at* http://www.europa.eu.int/comm/internal_market/privacy/index_en.htm (last visited Jan. 10, 2005).

13. Directive 95/46, *supra* note 11, art. 3, para. 2. *See also* Andrew Charlesworth, *Data Privacy in Cyberspace: Not National vs. International but Commercial vs. Individual*, *in* LAW & INTERNET: A FRAMEWORK FOR ELECTRONIC COMMERCE 89–90 (Lilian Edwards & Charlotte Waelde eds., 2d ed. 2000).

14. 18 U.S.C. § 2510 *et seq.* (2000) (Wire and Electronic Communications Interception and Interception of Oral Communications).

15. *See infra* note 302.

limit such monitoring because private parties in the United States largely do not trust the government to intervene.

Part II of the Article presents the scheme of employee-privacy protection in the context of e-mail monitoring by an employer in Western Europe. It posits that while Directive 95/46 and other instruments attempt to protect employee privacy, the jurisprudence seems to undermine that protection. Part III of the Article describes the scheme of employee privacy protection in the context of e-mail monitoring by an employer in the United States. It compares the United States scheme with its European counterpart and concludes that the level of employee privacy protection is similarly low in both Western Europe and the United States.

Part IV of the Article considers the factors that are likely to determine the future of employee privacy protection. After describing the value of the right to privacy and the role of the government in the United States and Western Europe, it theorizes as to the future of employee privacy protection in the private sector in both regions based on these factors, and based on recent events in France and the United States.

II. APPROACH OF WESTERN EUROPE

The constitutions of Western Europe protect a private person from the government, but not from another private person.[16] Thus, various legal instruments that deal with data protection[17] in the private sector, including Directive 95/46, are important sources for analyzing employer monitoring of employee e-mail in the private sector. Case law addressing privacy issues in the workplace is helpful as well. However, while various legal instruments attempt to increase employee data protection, case law does not reflect this attitude.

A. Historical Development of Data Protection Law in Western Europe

Western European countries began to adopt national laws on privacy when faced with the technological development of the 1960s.[18] Sweden

16. *Cf.* Manfred Weiss & Barbara Geck, *Worker Privacy in Germany*, 17 COMP. LAB. L.J. 75, 75–76 (1995–96).

17. In Europe, the term designating information privacy is "data protection." Data protection refers to policies designed to regulate the collection, storage, use, or dissemination of personal information. This term is a translation of a German word *Datenschultz*. Patrick J. Murray, *The Adequacy Standard under Directive 95/46/EC: Does U.S. Data Protection Meet This Standard?*, 21 FORDHAM INT'L L.J. 932, 942 (1998).

18. COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 12–14 (1992).

adopted the first national data protection law in 1973.[19] Germany adopted a federal data protection law in 1977,[20] and France followed in 1978.[21] These European data protection laws covered both the public and private sectors[22] and regulated a wide range of activities, "including data collection, storage, use, and dissemination."[23] Moreover, they typically set up a third-party board to control the flow of data.[24]

However, these laws differed from one another in significant respects. In Sweden and France, for example, the laws gave the national data boards "sweeping authority to grant or deny authorization for public and private data processing."[25] Conversely, the national data board in Germany lacks the authority to issue binding opinions and has only an advisory function.[26]

---

19. Data Act of 1973 (as amended with effect from Jan. 1, 1989) (Swed.), http://elj.warwick.ac.uk/jilt/dp/material/dataact.htm (last visited Nov. 16, 2004) [hereinafter Swedish Data Act of 1973]. *See also* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 32 (1997) [hereinafter CATE, PRIVACY IN THE INFORMATION AGE]; DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 93 (1989) (presenting a detailed explanation of the background, contents, and problems of the Data Act of 1973).

20. *Bundesdatenschutzgesetz* [Federal Data Protection Act], v.27.1.1977 (BGBl. I, S. 201) [hereinafter 1977 BDSG]. The starting point of data protection in Germany was the Data Privacy Act, enacted by the State of Hesse in 1970, which preceded the Swedish data protection law. The German law was enacted as a response to concerns about the social implications of automated data processing in the public administration. However, it took seven years from the time of the enactment of the Hessen Data Privacy Act for the German government to enact a federal data protection law. There are several reasons why the process took so long. First, the regulation of data transfers within the federal government and the need for an independent supervisory agent were issues that had to be faced; second, the computer industry "won an extension of the law to manual files on individuals that are readily accessible for repeated uses"; third, there were "contention[s] from a variety of sectors that provisions in various special laws already offered a great deal of data protection and that no further external regulation or supervision was required." FLAHERTY, *supra* note 19, at 21–22, 24.

21. Law No. 78-17 on Informatics and Freedoms of Jan. 6, 1978, J.O., Jan. 6, 1978, *available at* http://www.legifrance.gouv.fr/texteconsolide/PPEAU.htm (last visited Jan. 21, 2005) [hereinafter French Data Protection Law of 1978]. By 1997, all the member states of the European Union except Greece had broad privacy or data protection statutes. CATE, PRIVACY IN THE INFORMATION AGE, *supra* note 19, at 32.

22. *See* Kristie A. Deyerle, *Genetic Testing in the Workplace: Employer Dream, Employee Nightmare—Legislative Regulation in the United States and the Federal Republic of Germany*, 18 COMP. LAB. L.J. 547, 591 (1997) (discussing the 1977 BDSG). *See also* FLAHERTY, *supra* note 19, at 94, 95, 169 (explaining that the Swedish model covering both public and private-sectors had an influence on the French Data Protection Law of 1978).

23. CATE, PRIVACY IN THE INFORMATION AGE, *supra* note 19, at 32.

24. In Germany, the federal law created an independent Data Protection Commissioner (DPC), who, by advising the federal government and individual ministers, ensured that the 1977 BDSG was implemented. *See* FLAHERTY, *supra* note 19, at 21. In Sweden, the Swedish Data Act of 1973 instructs the Data Inspection Board (DIB) to pay special attention to the nature and quantity of the personal data being collected, how and from whom the data is being acquired, and the attitudes of the data subjects. *Id*. at 93. France created the National Commission on Informatics and Freedoms (CNIL) to implement the French Data Protection Law of 1978. CNIL makes decisions on the authorization of particular information systems in response to requests from both the public and private-sectors. *Id*. at 165.

25. CATE, PRIVACY IN THE INFORMATION AGE, *supra* note 19, at 33. *See generally* FLAHERTY,

While these national laws contributed to data protection in the private-sector, they risked compromising the free flow of data because they established sometimes conflicting regimes for data protection in the various states. For example, Sweden refused to recognize a British corporation contract for the manufacture of a card with a magnetic strip capable of storing data, because Sweden believed British law did not sufficiently protect privacy.[27] Given the increase in the transnational flow of personal data in the 1970s that created greater interdependence among European countries, Sweden's refusal demonstrated a serious problem. As a result, Western Europe faced the difficult task of harmonizing personal data legislation.

In the early 1980s, two major multinational data protection agreements attempted to harmonize these disparate national laws.[28] In 1980, the Organisation for Economic Co-Operation and Development (OECD) adopted the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.[29] One year later, the Council of Europe promulgated the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[30] Both the OECD Guidelines and the Council of Europe Convention define "personal data" broadly as "any information relating to an identified or identifiable individual."[31] "Data controller" in the OECD Guidelines and "controller of the file" in the Council of Europe Convention cover a broad range of parties as well.[32] Both explicitly cover public and private sectors[33] and set

---

supra note 19, at 112–25 (discussing the powers of the DIB).

26. CATE, PRIVACY IN THE INFORMATION AGE, *supra* note 19, at 33; BENNETT, *supra* note 18, at 182. *See generally* FLAHERTY, *supra* note 19, at 40–47 (discussing the powers of the DPC).

27. Solveig Singleton, *Privacy and Human Rights: Comparing the United States to Europe*, CATO INSTITUTE, Dec. 1, 1999, *at* http://www.cato.org/pubs/wtpapers/991201paper.html (last visited Nov. 16, 2004).

28. MURRAY, *supra* note 17, at 951–52.

29. OECD, *The Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, Sept. 23, 1980, *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (last visited Jan. 10, 2005) [hereinafter OECD Guidelines].

30. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, Europ. T.S. No. 108, *available at* http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm (last visited Sept. 9, 2004) [hereinafter Council of Europe Convention].

31. OECD Guidelines, *supra* note 29, para. 1(b). *See also* Council of Europe Convention, *supra* note 30, art. 2.

32. *See* OECD Guidelines, *supra* note 29, para. 1(a). Under the OECD Guidelines, "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether such data are collected, stored, processed or disseminated by that party or by an agent on its behalf. *See also* Council of Europe Convention, *supra* note 30, art. 2. Under the Council of Europe Convention, "controller of the file" means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data

forth policies on data collection, use, storage, and transmission, as well as with regard to the dissemination of personal information.[34]

However, the OECD Guidelines and the Council of Europe Convention failed to harmonize divergent national data protection laws in Europe because they permitted broad variation in national implementation.[35] First, the former required only voluntary adherence.[36] Conversely, the latter, with a greater focus on the importance of data protection to the right of privacy, established a minimum level of protection that signatories had to implement.[37] Unfortunately, this minimum level of protection did not

---

should be stored, and which operations should be applied to them. *Id.*

33. *See* OECD Guidelines, *supra* note 29, para. 2; Council of Europe Convention, *supra* note 30, art. 3, para. 1.

34. Joel R. Reidenberg, *The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services*, 60 FORDHAM L. REV. S137, S145 (1992); Michael P. Roch, *Filling the Void of Data Protection in the United States: Following the European Example*, 12 COMPUTER & HIGH TECH. L.J. 71, 74, 76 (1996). *See* OECD Guidelines, *supra* note 29, paras. 7–19. The OECD Guidelines put a limitation on the collection of personal data and the method of such collection, and provide that personal data should be relevant to the purpose for which they are to be used. To the extent that data collection is necessary for those purposes, it should be accurate, complete and up-to-date. Under the OECD Guidelines, the purpose of data collection must be specified and such specification is binding. Personal data should not be disclosed unless there is consent or authority of law. *See also* Council of Europe Convention, *supra* note 30, art. 5.

> Personal data undergoing automatic processing shall be:
>
> (a) obtained and processed fairly and lawfully;
>
> (b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
>
> (c) adequate, relevant and not excessive in relation to the purposes for which they are stored;
>
> (d) accurate and, where necessary, kept up to date;
>
> (e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Id. Additionally, both the OECD Guidelines and the Council of Europe Convention give individuals additional safeguards, including the right to inquire what data the controller has collected regarding the individual, and the right to ask for correction or erasure. OECD Guidelines, *supra* note 29, para. 13; Council of Europe Convention, *supra* note 30, art. 8.

35. Fred H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431–32 (1995) [hereinafter Cate, *The EU Data Protection Directive*].

36. OECD Guidelines, *supra* note 29, para. 19; *see also* Reidenberg, *supra* note 34, at S144.

37. Council of Europe Convention, *supra* note 30, art. 4.

> 1. Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.
>
> 2. These measures shall be taken at the latest at the time of entry into force of this convention in respect of that Party.

Id. See also OECD Guidelines, *supra* note 29, para. 19.

> In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:
>
> (a) adopt appropriate domestic legislation;
>
> (b) encourage and support self-regulation, whether in the form of codes of conduct or

harmonize national laws because the signatories set up different standards of data protection beyond the minimum level required by the Convention.[38] Second, "the Council of Europe Convention did not include definitions for important terms, such as what constitutes an 'adequate' level of data protection"[39] and, as a result, data protection laws in different countries had inconsistent definitions.[40] Third, harmonization was problematic because some European countries did not even ratify the Council of Europe Convention and, thus, the Convention had no effect on their national laws.[41]

In the meantime, the Council of Europe Committee of Ministers adopted a recommendation in 1989[42] mandating that employee privacy be

---

otherwise;

(c) provide for reasonable means for individuals to exercise their rights;

(d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and

(e) ensure that there is no unfair discrimination against data subjects.

Id. The OECD and the Council of Europe have different philosophies. The former is designed to foster economic growth among industrialized nations, while the latter's mission is to advance human rights. Thus, the OECD Guidelines emphasize the importance of the free flow of information and provide for voluntary adherence, whereas the Council of Europe Convention stresses the need to protect individuals and obligates signatories to enact conforming national legislation. Reidenberg, *supra* note 34, at S144.

38. CATE, PRIVACY IN THE INFORMATION AGE, *supra* note 19, at 35; REIDENBERG, *supra* note 34, at S144 (providing examples of sensitive data, such as race, health and sexual preferences, or information regarding activities). The varying standards of protection reflect differing views on the nature of data privacy. Some countries, like Germany, France and the Nordic countries, put an emphasis on human rights whereas others, such as the United Kingdom, were afraid of disrupting international trade by setting up a standard beyond the minimum requirement of the Council of Europe Convention. Charlesworth, *supra* note 13, at 85.

39. CATE, PRIVACY IN THE INFORMATION AGE, *supra* note 19, at 35.

40. *Id*.

41. By 1992, only ten countries—Denmark, France, Germany, Ireland, Luxembourg, Spain and the United Kingdom (seven of twelve European Community member states as of 1992) plus Austria, Norway and Sweden—had ratified the Council of Europe Convention. On the other hand, eight countries—Belgium, Greece, Italy, the Netherlands, Portugal (five of twelve European Community member states) plus Cyprus, Iceland and Turkey—had signed without ratification. *Id*. at 34, 35.

42. Council of Europe Recommendation, *supra* note 10. Article 1.1 of the Council of Europe Recommendation makes clear that the recommendation applies to the private and public-sectors. *Id*. art. 1.1. "Personal data" is defined similarly in the Council of Europe Convention, although there is a caveat that may limit the scope of personal data. Article 1.3 of the Council of Europe Recommendation provides: "The expression 'personal data' covers any information relating to an identified or identifiable individual. An individual shall not be regarded as 'identifiable' if identification requires an unreasonable amount of time, cost and manpower." *Id*. art. 1.3. There is also a comprehensive definition of "employment purposes."

> The expression "employment purposes" concerns the relations between employers and employees which relate to recruitment of employees, fulfilment of the contract of employment, management, including discharge of obligations laid down by law or laid down in collective agreements, as well as planning and organisation of work.

Id.

safeguarded by limiting employers' power to collect and store employee data.[43] According to the recommendation, the data collected must be relevant and not excessive in light of the employer's reasons for collecting it.[44] The recommendation also places limits on the sources from which data can be monitored.[45] Moreover, if the employer stores the data, it should be accurate, "up-to-date and represent faithfully the situation of the employee."[46] Additionally, the employer should not keep the data for a longer period than is justified by the purpose of data collection.[47]

The recommendation calls for additional safeguards for the collection and storage of certain sensitive data and requires explicit consent where no domestic law safeguards exist.[48] Employees ("data subjects") have a right to access all data collected by the employer and to have such data rectified or erased when contrary to principles set out in the Recommendation.[49]

Overall, while Western Europe made efforts to protect data and employee privacy in the private workplace, its attempts to protect data privacy did not assure the free flow of personal data within the region.

B. Directive 95/46

1. Development and Contents

By the early 1990s, the European Commission had confirmed that it was necessary to harmonize the standard of data protection within European Community member states.[50] The Commission began to regard the different standards afforded by member states' data protection laws as

---

43. *Id*. art. 2.1.

44. *Id*. arts. 4.2, 5.1.

45. Employers should collect personal data from the data subject. The data subject should be informed when the employer collects data from sources outside the employment relationship. *See id*. art. 4.1. In the context of recruitment, employers can use outside sources only when the data subject gives consent or is informed in advance. *See id*. art. 4.3.

46. *Id*. art. 5.2.

47. *Id*. art. 14.1.

48. Article 10.1 of the Council of Europe Recommendation provides:

> Personal data relating to racial origin, political opinions, religious or other beliefs, sexual life or criminal convictions referred to in Article 6 of the Convention for the protection of individuals with regard to automatic processing of personal data, should only be collected and stored in particular cases within the limits laid down by domestic law and in accordance with appropriate safeguards provided therein. In the absence of such safeguards, such data should only be collected and stored with the express and informed consent of the employees.

Id. art. 10.1. Additionally, there are safeguards for the collection of health data. *See id*. arts. 0.2-10.6.

49. *Id*. art. 12.1.

50. Charlesworth, *supra* note 13, at 85; CATE, PRIVACY IN THE INFORMATION AGE, *supra* note 19, at 35.

a potentially serious impediment to the implementation of its Single Market policy,[51] which requires the free movement of persons, goods, and services between member states.[52] Competition in the service industries of member states tempted those with stricter data protection laws to inhibit the movement of data from states with more lenient data protection laws to protect their own developing national industries and interests.[53] Additionally, member states with stricter data protection laws blocked the transfer of information to member states with more lenient laws.[54]

After long negotiations, the European Parliament and the European Union Council adopted Directive 95/46 in October 1995 to harmonize the standard of data protection within European Union member states and to confirm the importance of data protection.[55] Sweeping broadly, Directive 95/46 declares that member states have a duty to protect fundamental human rights, the freedom of natural persons, and the right to privacy in personal data in particular.[56] It pertains to "the processing of personal data

---

51. Charlesworth, *supra* note 13, at 85.

52. TREATY ESTABLISHING THE EUROPEAN ECONOMIC COMMUNITY, Mar. 25, 1957, 298 U.N.T.S. 3, arts. 9, 48, 59, *amended by* TREATY ESTABLISHING THE EUROPEAN COMMUNITY, Feb. 7, 1992, 1 C.M.L.R. 573 (1992) [hereinafter EEC TREATY]. Current provisions for freedom of goods, persons and services are found, respectively, in articles 23, 39 and 49. TREATY ESTABLISHING THE EUROPEAN COMMUNITY, Nov. 10, 1997, O.J. (C 340) 1 (1997), *available at* http://europa.eu.int/eur-lex/en/treaties/dat/C_2002325EN.003301.html (visited on Jan. 10, 2005) [hereinafter EC TREATY].

53. Charlesworth, *supra* note 13, at 85–86. The preamble to the Directive implies the existence of such a problem. Directive 95/46, *supra* note 11, pmbl., para. 9.

54. P. Amy Monahan, *Deconstructing Information Walls: The Impact of the European Data Directive on U.S. Businesses*, 29 LAW & POL'Y INT'L BUS. 275, 285 (1998); Jennifer L. Kraus, *On the Regulation of Personal Data Flows in Europe and the United States*, 1993 COLUM. BUS. L. REV. 59, 71 (1993) (stating that France did not allow the parent company of Fiat, located in France, to transmit employee career data to its subsidiary in Italy because Italy did not have any data protection laws and had not ratified the European Convention); Jennifer M. Myers, *Creating Data Protection Legislation in the United States: An Examination of Current Legislation in the European Union, Spain, and the United States*, 29 CASE W. RES. J. INT'L L. 109, 123 n.97 (1997) (pointing out that France had blocked the transfer to Spain of personal data concerning the identities of former Spanish Civil War prisoners who resided in France).

55. The preamble of Directive 95/46 refers to the necessity of harmonization. Directive 95/46, *supra* note 11, pmbl., paras. 7–9. The first paragraph of article 1 asserts the importance of data protection. *Id*. art. 1, para. 1. The road to the Directive was long and winding. The European Commission issued the initial draft in 1990, but it took five years and several drafts to adopt the final version of the Directive. Divergent attitudes toward data protection among the member states fueled the lengthy negotiations. *See* Charlesworth, *supra* note 13, at 86–87; CATE, PRIVACY IN THE INFORMATION AGE, *supra* note 19, at 35–36; Roch, *supra* note 34, at 79–88.

56. Directive 95/46, *supra* note 11, pmbl., paras. 10–11 & art. 1, para 1. In fact, the Directive tries to balance two competing values: the free flow of information and the right to privacy. Murray, *supra* note 17, at 959. The Directive provides that "Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1." (Paragraph 1 refers to the fundamental rights and freedoms of natural persons). Directive 95/46, *supra* note 11, art. 1, para. 2.

On the other hand, paragraph 10 of the Preamble provides:

wholly or partly by automatic means"[57] in both the public and private sectors.[58] Directive 95/46 creates exceptions only where the relevant data processing lies outside the scope of European Union law, such as in public security and law enforcement.[59] Directive 95/46 also excludes data processing for an individual's purely personal or household activities from the reach of data monitoring.[60] Such activities as the maintenance of an electronic personal diary or an address book with the names and telephone numbers of friends cannot be monitored.[61]

The broad definitions of the terms "personal data" and "processing of personal data" indicate the far-reaching application of Directive 95/46. "Personal data" means "any information relating to an identified or identifiable natural person ('data subject')."[62] This definition is almost identical to the definition of "personal data" in the OECD Guidelines and the Council of Europe Convention. The definition of "processing of personal data" (processing) is "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure

---

> Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

Directive 95/46, *supra* note 11, pmbl., para. 10. This paragraph prevents member states from sacrificing the right to privacy in order to achieve the free flow of information. Murray, *supra* note 17, at 959.

57. Directive 95/46, *supra* note 11, art. 3, para. 1.

58. European Commission, *supra* note 12.

59. Directive 95/46, *supra* note 11, art. 3, para. 2; Charlesworth, *supra* note 13, at 87. Public security and law enforcement are domains regulated by member states. *See* Directive 95/46, *supra* note 11, art. 13.

60. European Commission, *supra* note 12; Jordan M. Blanke, *"Safe Harbor" and the European Union's Directive on Data Protection*, 11 ALB. L.J. SCI. & TECH. 57, 62 (2000).

61. *Id.*

62. "An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." Directive 95/46, *supra* note 11, art. 2(a). This definition of "'personal data' potentially covers a wide range of types of information, including but not limited to, text, photographs, audiovisual images, and sound recordings of identifiable individuals." Charlesworth, *supra* note 13, at 87.

or destruction."[63] Thus, Directive 95/46 covers every facet of personal data processing.[64]

Directive 95/46 regulates the method of processing of personal data. Many of its principles follow those already set forth in the OECD Guidelines and the Council of Europe Convention.[65] Under Directive 95/46, personal data must be "processed fairly and lawfully."[66] The collection of personal data must have a specified purpose that is explicit, legitimate, and limited by the type of data collected and the uses to which it will be put.[67] Data must be accurate, up-to-date, adequate, relevant, and not excessive in relation to the purpose for which it is processed.[68] Article 7 of Directive 95/46 provides criteria for the legitimate processing of personal data.[69] Additionally, as to sensitive personal data, such as "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life," explicit consent by a data subject is required for the processing.[70]

Directive 95/46 also obliges data controllers to give data subjects certain information, including the identity of the controller, the purposes of the processing, and any further information necessary to guarantee fair processing for the data subject.[71] Additionally, Directive 95/46 gives each data subject the right to access their data[72] and the right to object to the processing of their personal data.[73] Finally, automated data processing cannot be the sole basis for decisions that significantly affect data subjects in most cases.[74]

---

63. Directive 95/46, *supra* note 11, art. 2(b).

64. Charlesworth, *supra* note 13, at 87.

65. As for the principles set forth in the OECD Guideline and the Council of Europe Convention, *see supra* notes 29, 30, 34 and accompanying text.

66. Directive 95/46, *supra* note 11, art. 6(a).

67. *Id*. art. 6(b).

68. *Id*. arts. 6(c), 6(d).

69. *Id*. art. 7.

70. *Id*. art. 8.

71. Articles 10 and 11 of Directive 95/46 outline what information a data controller must give to a data subject. Article 10 applies when data is collected from a data subject, and article 11 applies when data has not been obtained from the data subject. Neither article, however, requires a data controller to provide such information when the data subject already has it. *See id*. arts. 10, 11.

72. *Id*. art. 12. This indicates that anyone is entitled to approach any data controller to inquire whether the controller processes personal data relating to the data subject, to receive a copy of the data, and if need be, to request that the data be erased. In such cases, the data subject may also require the data controller, where possible, to notify third parties who had previously consulted the incorrect data. European Commission, *Data Protection*, *supra* note 12.

73. Directive 95/46, *supra* note 11, art. 14. The right to object includes a right to object to the lawful processing of one's personal data, as well as a right to object to such processing for the purpose of direct marketing. *Id*. *See also* Charlesworth, *supra* note 13, at 87.

74. Decisions that significantly affect the data subject, such as the decision to grant a loan or

To enforce the data protection rules, Directive 95/46 obliges each member state to create a national supervisory authority.[75] This authority has the power to investigate any processing of personal data that may affect the rights and freedoms of data subjects. They also have the power to order erasure of data, to require cessation of processing, and to block proposed transfers of data to third parties.[76] A national supervisory authority further has the power to engage in legal proceedings when there is a violation of a national data protection law that implements the Directive.[77] Additionally, Directive 95/46 has sections regarding liability, sanctions, and remedies in case of a violation.[78]

The most controversial portion of Directive 95/46 is article 25, which restricts the transfer of personal data to a third country that does not have an adequate level of data protection.[79] The evaluation of adequacy takes into consideration all the circumstances surrounding a data transfer operation or set of operations.[80] The United States feared that article 25 might interrupt the free flow of information from the European Union to the United States, thereby hampering the ability of American companies to engage in trans-Atlantic transactions.[81] Therefore, in 2000, the European

---

issue insurance, could theoretically be made on the sole basis of automated data processing. Under the Directive, this can only be done in the course of entering or performing a contract. In this situation, the data controller must adopt suitable safeguards. For instance, the data controller could allow the data subject to protest if her requests are not satisfied. Other types of automated decisions might be authorized by statute. European Commission, *Data Protection*, *supra* note 12.

75. Directive 95/46, *supra* note 11, art. 28, paras. 1, 2.

76. *Id*. art. 28, para. 3; CATE, PRIVACY IN THE INFORMATION AGE, *supra* note 19, at 40.

77. Directive 95/46, *supra* note 11, art. 28, para. 3.

78. *Id*. arts. 22–24.

79. *Id*. art. 25.

80. Article 25 of the Directive provides:

> The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

Id. art. 25, para. 2. However, there are some narrow exceptions to this rule in article 26, including: unambiguous consent; transfer necessary for the performance of a contract where the data subject or her interest is involved; transfer necessary or legally required on important public interest grounds; and transfer necessary to protect the vital interests of the data subject. *Id*. art. 26, para. 1.

81. *See* CATE, PRIVACY IN THE INFORMATION AGE, *supra* note 19, at 127. For an explanation of why scholars believed article 25 might interrupt the free flow of information between the European Union and the United States, see Laura A. Bischoff, *Technology Makes Gathering, Storing and Disseminating Personal Information about You and Your Habits Extremely Easy . . . and That's Not Always Good*, THE DAYTON DAILY NEWS, June 6, 1999, at 1F, *available at* LEXIS, News Library, DDN File. United States Department of Commerce, *Safe Harbor: Safe Harbor Overview*, *at* http://www.export.gov/safeharbor/sh_overview.html (last visited Nov. 16, 2004). Whether the United

Union and the United States agreed to create a "safe harbor" framework, which allows American companies to comply with the directive's adequacy requirement.[82]

States satisfies the adequacy requirement of the Directive is a hotly debated issue. *See generally* Cate, *The EU Data Protection Directive*, *supra* note 35, at 437–39 (casting doubts on adequacy of the protection of privacy in the United States); Monahan, *supra* note 54, at 287–93 (implying the inadequacy of the standard in the United States by stating that the Directive would force the United States to make at least some changes in its data protection law); Roch, *supra* note 34 (taking a position that the United States clearly did not meet the adequacy standard set by the Directive); Graham Pearce & Nicolas Platten, *Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective*, 22 FORDHAM INT'L L.J. 2024, 2039–47 (1999); Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 22–38 (2000); Murray, *supra* note 17 (examining the adequacy of the U.S. scheme in detail and suggesting that many areas of public sector and some areas of private-sector met the adequacy requirement while many areas of private-sector, such as health care and direct marketing, failed to meet the adequacy requirement).

82. Under the "safe harbor" framework, a company is deemed to satisfy the adequacy requirement of the Directive if the company satisfied the following seven principles:

> 1. Notice: Organizations must notify individuals of the purposes underlying their collection and usage of personal data. They must provide information on how individuals can contact the organization with any inquiries or complaints, the types of third parties to whom it discloses their data, and the choices and means the organization offers for limiting the use and disclosure of their data.
>
> 2. Choice: Organizations must give individuals the opportunity to choose (opt out) whether their personal data will be disclosed to a third party or used in a way incompatible with the purpose underlying its original collection or subsequent authorization by the individual. For sensitive information, affirmative or explicit (opt in) consent must be given for the information to be disclosed to a third party or used for a purpose other than its original purpose or a purpose authorized subsequently by the individual.
>
> 3. Onward Transfer (Transfers to Third Parties): To disclose information to a third party, organizations must satisfy the notice and choice requirements. Additionally, when the third party transferee is acting as an agent(1), the organization may transfer the information if it makes sure that the third party either subscribes to the safe harbor principles or is subject to Directive 95/26 or another adequacy finding. Alternatively, the organization can enter into a written agreement with the third party requiring the third party provide at least the same level of privacy protection as is required by the relevant principles.
>
> 4. Access: Individuals must have access to the personal information held by an organization on them. They must also be able to correct, amend, or delete that information when it is inaccurate. However, there are exceptions when the burden or expense of providing access would be disproportionate to the risks to the individual's privacy and when granting access would violate the rights of persons other than the individual.
>
> 5. Security: Organizations must take reasonable precautions to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction.
>
> 6. Data integrity: Personal information must be relevant to the purposes for which it will be used. An organization should take reasonable steps to ensure that data is reliable, accurate, complete, and current.
>
> 7. Enforcement: To ensure compliance with the "safe harbor" principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints can be investigated and resolved and damages awarded where the applicable law or private-sector initiatives so provide; (b) procedures for verifying implementation of the commitments companies make to adhere to the safe harbor principles; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be

Directive 95/46 provides that the victim of a violation of the Directive is entitled to compensation from the controller for damages suffered. However, it does not specify any criminal punishment for a violation. Rather, each member state must legislate sanctions, including criminal punishment, to address such violations.[83]

As mentioned, Directive 95/46 offers a general framework for the protection of the right to privacy. However, whether Directive 95/46 actually protects a data subject depends on how article 7 is interpreted. A broad interpretation of article 7, which sets forth justification for data processing, would undermine the right of a data subject to privacy. Among the justifications listed, article 7(f) and article 7(a) appear to be relevant in light of the typical motives of employers that conduct e-mail monitoring.[84]

Article 7(a) plays a limited role. First, according to the provision, consent must be unambiguous.[85] Second, "the data subject's consent" under Directive 95/46 is defined as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."[86] Under this definition, an employee has given consent consistent with article 2(h) and article 7(a) only when that employee can withdraw consent without prejudice.[87] However, it is nearly impossible to imagine a situation where an employee would be able to withdraw consent without prejudice when

---

> sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self-certification letters will no longer appear in the list of participants, and safe harbor benefits will no longer be assured.

United States Department of Commerce, *supra* note 81. For an academic discussion of the "safe harbor" framework, see James T. Sunosky, *Privacy Online: A Primer on the European Union's Directive and United States' Safe Harbor Privacy Principles*, CURRENTS INT'L TRADE L.J., Winter 2000, at 86–88; Jordan M. Blanke, *supra* note 60; Sean D. Murphy, *Contemporary Practice of the United States Relating to International Law: Legal Regulation of Information*, 95 AM. J. INT'L L. 132, 156–59 (2001); James M. Assey, Jr. & Demetrios A. Eleftheriou, *The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters?*, 9 COMMLAW CONSPECTUS 145, 151–53 (2001); Anna E. Shimanek, *Do You Want Milk with Those Cookies?: Complying with the Safe Harbor Privacy Principles*, 26 IOWA J. CORP. L. 455, 471–76 (2001); Julia Gladstone, *The Impact of E-Commerce in the Laws of Nations Article: The U.S. Privacy Balance and the European Privacy Directive: Reflections on the United States Privacy Policy*, 7 WILLAMETTE J. INT'L L. & DISPUTE RES. 10, 24–28 (2000); Charlesworth, *supra* note 13, at 109–19.

83. Directive 95/46, *supra* note 11, art. 24.

84. *Id.* arts. 7(a) and 7(f).

85. *Id.* art. 7(a).

86. *Id.* art. 2(h).

87. THE ARTICLE 29 WORKING PARTY, OPINION 8/2001 ON THE PROCESSING OF THE PERSONAL DATA IN THE EMPLOYMENT CONTEXT 23 (2001), *available at* http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2001/wp48en.pdf (last visited Jan. 10, 2005) [hereinafter ARTICLE 29 WORKING PARTY]. The Article 29 Working Party is an organization established by European Union Directive 95/46 designed to function as an independent advisory board relating to matters of data protection and privacy. *Id.*

an employer is monitoring in order to protect their own computer system, networks, and trade secrets.

Article 7(f) plays a far greater role than article 7(a). According to article 7(f), data processing, without the unambiguous consent of the data subject, is possible if there are "legitimate" interests pursued by the controller or by the third party or parties to whom the data is disclosed.[88] This provision balances the interests served by the processing of data (the interests of employers in workplace e-mail monitoring) and the right to privacy (the interest of employees).[89] Such a balancing test carries a risk, even though the data subject has a right to object to the processing of data under certain circumstances.[90] This risk exists, in particular, in member states that interpret broadly the term "legitimate."[91] As the interpretation of this relatively new directive has not yet developed in the courts of the European Community, it is necessary to look at existing European case law.

2. Implementation of Directive 95/46

a. Implementation Process

Directive 95/46 requires member states to adopt national implementing laws.[92] Because member states may offer greater protection than the Directive mandates through domestic laws, standards of protection may differ among member states.[93] Despite these differences, however, member states cannot limit the free flow of information to other member states, as this would frustrate one of the stated purposes of the Directive.[94]

---

88. Directive 95/46, *supra* note 11, art. 7(f).

89. *Id*.

90. Directive 95/46, *supra* note 11, art. 14.

91. "While the operative legal concepts of article 7(a) (collection with consent) and article 7(b) (in preparation or performance of a contract) are fairly definite, those of article 7(f) are considerably more indefinite. The Directive offers scant guidance in determining what interests are legitimate under article 7(f) and when they might be overridden by the interests of the data subject." James R. Maxeiner, *Freedom of Information and the EU Data Protection Directive*, 48 FED. COMM. L.J. 93, 99 (1995). A lack of clarity may allow a lenient interpretation in favor of various interests contrary to the right to privacy. PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 100 (1998) (stating, "[a]rticle 7(f) is potentially very expansive, because of the range of 'legitimate interests' that might justify processing personal information."). Good examples of how the balancing approach can lead to different conclusions include *Halford* and *Nikon France*, both of which are discussed *infra*.

92. European Commission, *Data Protection*, *supra* note 12.

93. Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 174, 191 (1999) [hereinafter Cate, *The Changing Face of Privacy*].

94. Directive 95/46, *supra* note 11, pmbl., paras. 7–8.

The implementation process in member states has been relatively slow. Although Directive 95/46 entered into effect on October 25, 1998,[95] only two member states, Greece and Italy, had implemented it by that time.[96] In July 1999, the European Commission sent reasoned opinions to nine member states (France, Luxembourg, the Netherlands, Germany, the United Kingdom, Ireland, Denmark, Spain, and Austria) for their failure to take all the measures necessary to implement Directive 95/46.[97] Five member states—France, Luxembourg, the Netherlands, Germany, and Ireland—still had not finished implementing Directive 95/46 by January 2000, when the European Commission took them to the European Court of Justice for this failure.[98] Since that time, five states have adopted laws implementing the Directive.[99]

---

95. Press Release, European Commission, Directive on Personal Data Protection Enters into Effect (Oct. 23, 1998), *at* http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/98/925&format=HTML&aged=1&language=EN&guiLanguage=en (last visited Nov. 16, 2004).

96. *Id*. Member states were supposed to have implemented the Directive 95/46 by October 24, 1998. *See* European Commission, *Data Protection*, *supra* note 12.

97. Press Release, European Commission, Data Protection: Commission Decided to Send Reasoned Opinions to Nine Member States (July 29, 1999), *at* http://europa.eu.intrapid/pressReleasesAction.do?reference=IP/99/592&format=HTML&aged=1&language=EN&guiLanguage=en (last visited Nov. 16, 2004).

Article 226, Paragraph 1 of the E.C. Treaty provides:

> If the Commission considers that a Member State has failed to fulfil an obligation under this Treaty, it shall deliver a reasoned opinion on the matter after giving the State concerned the opportunity to submit its observations.

EC TREATY, *supra* note 52, art. 226, para. 1.

98. Press Release, European Commission, Data Protection: Commission Takes Five Member States to Court (Jan. 11, 2000), *at* http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/00/10&format=HTML&aged=1&language=EN&guiLanguage=en (last visited Nov. 16, 2004).

Article 226, Paragraph 2 of the E.C. Treaty provides: If the State concerned does not comply with the opinion within the period laid down by the Commission, the latter may bring the matter before the Court of Justice. EC TREATY, *supra* note 52, art. 226, para. 2.

99. European Commission, *Status of Implementation of Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Data*, *at* http://europa.eu.int/comm/internal_market/privacy/law/implementation_en.htm (visited Nov. 16, 2004) [hereinafter Status of Implementation]. In the Netherlands, the Dutch parliament adopted *Wet bescherming persoonsgegevens* in July 2000. This law is designed to implement Directive 95/46. *See Wet bescherming persoonsgegevens* [Personal Data Protection Act], 6 juli 2000, NJ 302, *available at* http://www.justitie.nl/Images/11_5235.pdf (last visited Jan. 10, 2005). In Germany, six states (Brandenburg, Baden-Württemberg, Bayern, Hessen, Nordrhein-Westfalen, and Schleswig-Holstein) adopted state laws implementing Directive 95/46. At the federal level, the new version of *Bundesdatenschutzgesetz* v. 23.05.2001 (BGBl.I S.904), [Federal Data Protection Act], which applies to both the public and private-sector, was adopted on May 18, 2001 and took effect on May 23, 2001. *Id.* Ireland enacted the Data Protection (Amendment) Act 2003 on April 10, 2003 to implement Directive 95/46. Data Protection (Amendment) Act 2003, 6, 2003, *available at* http://www.dataprivacy.ie/images/Act2003.pdf (last visited Dec. 20, 2004). The Data Protection (Amendment) Act 2003 took effect on July 1, 2003. European Commission, *Status of Implementation*, *supra*. In August 2004, French Parliament adopted *Loi n° 2004-801 du 6 août 2004 relative á la protection des personnes physiques á l'égard des traitements de données á caractére personnel et*

b. Example of Implementation—Belgium

In 1998, Belgium implemented Directive 95/46 by modifying its 1992 national data protection law.[100] The 1992 Belgian Data Protection Law applied to the automatic processing of personal data and to manually processed files compiled and stored in a logical manner for systematic consultation.[101] Under this law, "automatic processing" meant any operation carried out wholly or in part by automatic means for recording, storing, modifying, erasing, consulting, or disseminating personal data.[102]

The 1992 law also established basic principles to regulate personal data processing. For example, the law impliedly included the principle of fair and lawful processing of personal data.[103] A data subject could request that data regarding them be deleted, or the subject may forbid the use of certain data if the data controller kept such data for a period longer than necessary.[104] The 1992 Belgian Data Protection Law also established the principle that personal data may only be processed for a specified and legitimate purpose.[105] According to *la Commission de la Vie Privée*

---

modifiant la loi nº 78–17 du 6 janvier 1978 relative á l'informatique, aux fichiers et aux libertés in order to implement the Directive. *Loi n 2004-801 du 6 août 2004 relative á la protection des personnes physiques á l'égard des traitements de données á caractére personnel et modifiant la loi n 78–17 du 6 janvier 1978 relative á l'informatique, aux fichiers et aux libertés* [Law No. 2004-801 of 6 August 2004 on the Protection of Natural Persons with regard to the Processing of Personal Data and Modifying Law No. 78–17 of 6 January 1978 on Data Processing, Files and Liberties], *available at* http://www.legifrance.gouv.fr/Waspad/UnTexteDeJorf?numjo=JUSX0100026L (last visited Feb. 24, 2005). In Luxembourg, *Loi du 2 août 2002 relative á la protection des personnes á l'égard du traitement des données á caractére personnel* was adopted in order to implement the Directive. *Loi du 2 août 2002 relative á proetection des personnes á l'égard du traitement des données á caractére personnel* [Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data], *available at* http://www.etat.lu/memorial/memorial/a/2002/a0911308.pdf (last visited Feb. 24, 2005). This law took effect on December 1, 2002. European Commission, *Status of Implementation*, *supra.*

100. *La Loi du 8 Décembre 1992 relative à la Protection de la Vie Privée à l'égard des Traitements de Données à Caractère Personnel, Modifiée par la Loi du 11 Décembre 1998* [Law of Dec. 8, 1992 on Privacy Protection in relation to the Processing of Personal Data, Modified by Law of Dec. 11, 1998], http://www.law.kuleuven.ac.be/icri/publications/499Consolidated_Belgian_Privacylaw_v200310.pdf (last visited Nov. 16, 2004) [hereinafter 1998 Belgian Data Protection Law]; *La Loi du 8 Décembre 1992 relative à la Protection des Données á Caractére Personnel* [Law of Dec. 8, 1992 on the Protection of the Processing of Personal Data], *available at* http://www3.dekamer.be/digidoc/DPS/K2332/K23321887/K23321887.pdf (last visited Feb. 2, 2005) [hereinafter 1992 Belgian Data Protection Law].

101. 1992 Belgian Data Protection Law, *supra* note 100, art. 1, paras. 1–2.

102. *Id*. art. 1, para. 3.

103. Sophie Louveaux, *Comments on the EU Data Protection Directive—The Belgian Perspective*, 2 J.INFO. L. & TECH., May 7, 1996, *at* http://elj.warwick.ac.uk/jilt/dp/2louveau/default.htm (last visited Dec. 20, 2004).

104. 1992 Belgian Data Protection Law, *supra* note 100, art. 12, para. 1.

105. *Id*. art. 5.

(Belgian Privacy Commission), whether a purpose is legitimate is determined by balancing interests through a process similar to the method found in article 7(f) of Directive 95/46.[106] The Belgian law also provided for transparency as a major principle by requiring that the data subject be informed of the recording of personal data.[107]

The 1998 Belgian Data Protection Law, in its amended form, closely followed Directive 95/46 and expanded the protections given to the data subject.[108] First, it extended the definition of "processing" to cover data collection[109] and made explicit the principle of fair and lawful processing of personal data.[110] Additionally, the 1998 law accorded a data subject the right to object to data processing for serious and legitimate reasons.[111]

C. Case Law

As of this Article's publication, no cases regarding employee privacy in the private-sector have reached the European Court of Justice, the judicial arm of the European Union, or the European Court of Human Rights, the judicial branch of the Council of Europe. However, because Directive 95/46 treats similarly the public and private-sectors, exploring cases from these courts regarding employee privacy in the public sector will be helpful. These cases indicate that the privacy of employees in the private-sector may not be protected to any great extent.

1. Tzoanos v. Commission of the European Communities

In *Tzoanos v. Commission*, the European Court of First Instance, a court subordinate to the European Court of Justice, took a minimalist approach to the right of privacy of public employees.[112] While working for the European Commission,[113] George Tzoanos used a computer owned by the European Commission for official purposes.[114] While he was out of his office, European Commission officers examined the computer's memory

106. Louveaux, *supra* note 103; *see also* Directive 95/46, *supra* note 11, art. 7(f).
107. 1992 Belgian Data Protection Law, *supra* note 100, art. 9.
108. *See generally* 1998 Belgian Data Protection Law, *supra* note 100; Directive 95/46, *supra* note 11.
109. 1998 Belgian Data Protection Law, *supra* note 100, art. 1, para. 2.
110. *Id*. art. 4, para. 1, sub-para. 1; *cf.* Directive 95/46, *supra* note 11, art. 6, para. 1(a).
111. 1998 Belgian Data Protection Law, *supra* note 100, art. 12, para. 1. *Cf.* Directive 95/46, *supra* note 11, art. 14.
112. Case T-74/96, Tzoanos v. Commission, 44 E.C.R. IA-00129, II-00343 (1998).
113. *Id.*
114. *Id.*

and found documents that would constitute a basis for disciplinary action.[115]

The European Court of First Instance found that the European Commission could examine the computer used by Tzoanos without his presence and use the information to commence a disciplinary action against him.[116] To justify its conclusion, the court first pointed out that the European Commission had always been the computer's owner and had allowed Tzoanos to use the computer exclusively for European Commission work.[117] The court then justified its conclusion through reliance on the duty of European Commission employees to serve the interests of the European Commission.[118]

2. Halford v. United Kingdom

The European Court of Human Rights dealt with the right to privacy in public-sector workplaces in *Halford v. United Kingdom*.[119] Alison Halford, Assistant Chief Constable with the Merseyside Police, had two telephone lines in her office, one of which was for private use.[120] These telephones were outside the public network and a part of the Merseyside police internal telephone network.[121] The Merseyside police placed no restrictions on the use of these telephones nor gave Halford any guidance on their use.[122]

After being denied a promotion several times, she commenced proceedings in 1990 in the Industrial Tribunal for gender discrimination.[123] Thereafter, she alleged that the Merseyside police intercepted her telephone calls to obtain information to use against her in the discrimination proceeding.[124]

The court rejected the government's argument that article 8 of the European Convention of Human Right (ECHR) did not protect telephone

115. *Id.*
116. *Id.*
117. *Id.*
118. *Id.*
119. Halford v. United Kingdom, 39 Eur. Ct. H.R. 1004 (1997).
120. *Id.* at 1009–10.
121. *Id.* at 1009–10. British law only applied to the public network. *See* Interception of Communications Act, 1985, c.56 (Eng.). Thus, the European Court of Human Rights directly applied article 8 of the ECHR. *See Halford*, 39 Eur. Ct. H.R. at 1014-20.
122. *Id.* at 1010.
123. *Id.* at 1009.
124. *Id.* at 1010.

calls by Halford from her office telephones because she had no reasonable expectation of privacy.[125] In rejecting this argument, the court noted:

> There is no evidence of any warning having been given to Ms. Halford, as a user of the internal telecommunications system operated at the Merseyside police headquarters, that calls made on that system would be liable to interception. She would, the Court considers, have had a reasonable expectation of privacy for such calls, which expectation was moreover reinforced by a number of factors. As Assistant Chief Constable she had sole use of her office where there were two telephones, one of which was specifically designated for her private use. Furthermore, she had been given the assurance, in response to a memorandum, that she could use her office telephones for the purposes of her sex-discrimination case . . . .[126]

While Halford won on the specific issue of the interception of office telephone calls, the court's decision did not necessarily lead to greater protection. The court merely held that an employer cannot monitor their employee's communications without advance notice, especially when the employer allowed employees to use office communication systems for private purposes.[127] This left room for a later holding that an employer may intercept employee communications if they give advance notice of the interception.[128]

Thus, in light of these two cases and the failure of Directive 95/46 to distinguish between the public and private sectors or between business and non-business hours, e-mail monitoring by an employer in the private-sector workplace may be allowed. As long as the employer gives advance notice of the interception to employees, neither the contents of the e-mail nor the time at which an employee sent the e-mail will prevent this monitoring.[129] On the other hand, if a private-sector employer allows employees to send personal e-mail, this authorization will limit their ability to monitor employee e-mail.

As a result, despite a comprehensive framework for data protection based on Directive 95/46, case law indicates that Western Europe does not

---

125. *Id.* at 1016.
126. *Id.*
127. *Id.*
128. *See infra* Part IV.B.
129. However, in France, it seems to be impossible for an employer to monitor employee e-mail sent during non-business hours. *See infra* Part IV.

necessarily protect the e-mail of private-sector employees against employer monitoring to any great extent.

III. THE UNITED STATES

While the U.S. Constitution protects the privacy of individuals from intrusions by the government, it does not protect their privacy against intrusions by another private person.[130] Thus, an employee's privacy is not constitutionally protected against intrusions by a private-sector employer.[131] Rather, private-sector employees must base their invasion of privacy claims on the Electronic Communications Privacy Act of 1986 (ECPA),[132] state statutes,[133] or state common law.[134]

While the ECPA sets up some privacy protection principles, it does not provide as much protection as Directive 95/46. Indeed the ECPA's exceptions tend to swallow its protections.[135] Additionally, state common law does not protect employees to a great extent, as in many cases it applies a standard arguably similar to that developed in European jurisprudence.[136] Finally, state statutes generally have weaknesses similar to those of the ECPA and state common law.

A. Historical Development of American Privacy Law in the Context of New Technology

During the 1970s, when technological developments caused Western Europe to adopt national laws regulating privacy in the private sector,

130. Charlesworth, *supra* note 13, at 92. There is an exception to this general rule when the actions of the nongovernmental entity can be fairly attributed to the State. Wilborn, *supra* note 9, at 828; Ronald J. Krotoszynski, Jr., *Back to the Briarpatch: An Argument in Favor of Constitutional Meta-Analysis in State Action Determinations*, 94 MICH. L. REV. 302, 306 (1995).

131. Wilborn, *supra* note 9, at 828. The Fourth Amendment protects people from unreasonable searches and seizures by the government. It does not, however, necessarily apply to searches performed by private parties. Anne L. Lehman, *E-Mail in the Workplace: Question of Privacy, Property or Principle?*, 5 COMMLAW CONSPECTUS 99, 100–01 (1997). For example, the Supreme Court found in *Burdeau v. McDowell* that the Fourth Amendment was not intended to apply to searches and seizures by parties other than governmental agencies. Burdeau v. McDowell, 256 U.S. 465, 475 (1921).

132. Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat 1848, 18 U.S.C. §§ 2510, 2521, 2701–10, 3117, 3121–26 (2000) [hereinafter ECPA]. The ECPA is the only federal statute that specifically addresses the interception and accession of e-mail communications. Gantt, *supra* note 9, at 351.

133. *See infra* Part III.C.1.

134. *See infra* Part III.C.2.

135. *See infra* Part III.B.2.

136. *See infra* Part III.C.2.

governmental abuses of power preoccupied the United States.[137] The U.S. public was concerned about the surveillance of war protestors during the Vietnam War[138] and the abuses of wiretapping powers (leading to the divulsion of tax, bank, and telephone records) revealed by the Watergate investigation.[139]

As a result of this preoccupation, the United States adopted the Privacy Act of 1974.[140] Under the Privacy Act, no governmental agency may disclose to any person or another agency by any means of communication any record contained in a system of records without the written request or prior consent of a person to whom the record pertains.[141] Additionally, an agency must keep data under its control accurate.[142] Individuals may access the data, and they have a right to correct it.[143] Finally, the Privacy Act requires agencies, when they collect data, to notify the individual of the collection and the reasons for it.[144]

Combined with the Freedom of Information Act,[145] the Privacy Act provides comprehensive information privacy in the public sector.[146] Moreover, the principles expressed in the Privacy Act mirror those expressed in most of the European data protection laws, including Directive 95/46.[147] However, unlike European data protection laws, the Privacy Act of 1974 only applies to the public sector.[148]

In the private sector, the United States has provided data protection through piecemeal legislation. Each act covers a specific field in the private sector, such as video privacy or electronic fund transfers.[149] The ECPA is the only law not limited to a specific field.[150] It is also the only

137. Singleton, *supra* note 27.
138. *Id.*
139. *Id*.
140. Privacy Act of 1974, 5 U.S.C. § 552a (2000).
141. 5 U.S.C. § 552a(b) (2000); Patricia I. Carter, *Health Information Privacy: Can Congress Protect Confidential Medical Information in the "Information Age"?*, 25 WM. MITCHELL L. REV. 223, 242 (1999).
142. 5 U.S.C. § 552a(c) (2000).
143. 5 U.S.C. § 552a(d) (2000); Carter, *supra* note 141, at 242.
144. 5 U.S.C. § 552a(g)(1) (2000); Carter, *supra* note 141, at 242.
145. 5 U.S.C. § 552 (2000).
146. Monahan, *supra* note 54, at 279.
147. *See supra* Part II.
148. 5 U.S.C. § 552a (2000).
149. *E.g.*, Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2000); Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3422 (2000); Fair Credit Reporting Act, 15 U.S.C. §§ 6721–39, 6791–66, 6781, 6801–09, 6821–27, 6901–10, 1681 (2000); Gramm-Leach-Bliley Act, 12 U.S.C. 24(a), 248(b), 1820(a), 1828, 1831, 6801 (2000); Electronic Fund Transfer Act, 15 U.S.C. § 1693 (§§).
150. The ECPA applies to the private-sector as a whole. *See generally* ECPA, *supra* note 132.

federal law relevant to employer monitoring of employee e-mail in the private sector.[151]

While the U.S. Congress attempted to enact a federal law to protect an employee's privacy in the private sector in both 1993 and 2000, those attempts failed.[152] In 1993, Senator Paul Simon introduced a bill called the Privacy for the Consumer and Worker Act.[153] This act required employers to clearly define their privacy policies; to refrain from monitoring personal communication and from video monitoring locker rooms and bathrooms; and to notify workers of telephone monitoring, unless it was for quality control.[154] Congress, however, shelved the act in 1994.[155]

In 2000, Congress attempted to pass the Notice of Electronic Monitoring Act,[156] which would have required employers to give employees advance notice of wire or network (including e-mail) monitoring.[157] It also would have required that notice be clear, conspicuous, and given annually or each time an employer's monitoring policy changed.[158] However, this law also did not pass.[159]

B. The Electronic Communications Privacy Act of 1986

In 1986, Congress adopted the ECPA by amending Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[160] Its intent was to address e-mail interception and access.[161] The ECPA prohibits certain types of monitoring and provides criminal sanctions for violators in an effort to protect the privacy of private persons. However, as will be shown, the ECPA's exceptions undermine its own privacy protections.

---

151. *Id.*

152. Electronic Privacy Information Center, *Workplace Privacy*, Aug. 3, 2004, *at* http://www.epic.org/privacy/workplace/default.html (last visited Nov. 17, 2004).

153. Privacy for Consumers and Workers Act, S. 984, 103d Cong. (1993).

154. *Id. See also* Roger Doyle, *Privacy in the Workplace*, 280 SCI. AM. 36 (1999), *available at* http://www.sciamarchive.org/qpdf.cfm?ArticleID_CHAR=EE1DC213-1F5E-41F3-ACDF-BE3D45F9EED (last visited Feb. 2, 2005).

155. *Id*.

156. Notice of Electronic Monitoring Act of 2000, H.R. 4908, 106th Cong. (2000) [hereinafter Notice of Electronic Monitoring Act of 2000]. *See also* Electronic Privacy Information Center, *supra* note 152.

157. Notice of Electronic Monitoring Act of 2000, *supra* note 156, § 2711(a); *see also* Sherry L. Travers, *Notice of Electronic Monitoring Act: 1984 Revisited?*, http://library.lp.findlaw.com/articles/file/00132/004846/title/subject/topic/constitutional%20law_privacy%20rights/filename/constitutionallaw_1_91 (last visited Nov. 17, 2004).

158. Notice of Electronic Monitoring Act of 2000, *supra* note 156, § 2711(b).

159. Travers, *supra* note 157.

160. Gantt, *supra* note 9, at 351.

161. *Id.*

1. The ECPA's Privacy Protections

The ECPA prohibits the unauthorized interception of electronic communications.[162] The definition of "intercept" under the ECPA includes non-aural acquisition, as the term is defined as the "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[163] In addition to interception, the ECPA prohibits breaking into an electronic storage system or intentionally exceeding authorized access.[164]

Although not clearly stated in the text,[165] the legislative history evidences a clear congressional intent to include e-mail within the ECPA's definition of electronic communications.[166] Additionally, case law demonstrates that the ECPA covers e-mail.[167] Nonetheless, the ECPA's overall scope of application seems narrower than that of Directive 95/46. While Directive 95/46 covers any processing of personal data, the ECPA only covers certain types of interception and access to electronic storage systems.

The ECPA seems implicitly to provide some of the principles explicit under the European data protection laws and Directive 95/46. For example, the ECPA's requirements that an interception be authorized and that access to an electronic storage system be within the range of such authorization indicate that the ECPA implicitly guarantees the principle of

---

162. 18 U.S.C. § 2511 (2000).

163. 18 U.S.C. § 2510(4) (2000).

164. 18 U.S.C. § 2701 (2000); Gantt, *supra* note 9, at 353.

165. The ECPA defines "electronic communication" as:

> (12) any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—
>
> (A) any wire or oral communication;
>
> (B) any communication made through a tone-only paging device;
>
> (C) any communication from a tracking device (as defined in section 3117 of this title); or
>
> (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

18 U.S.C. § 2510(12) (2000). *See also* Jarrod J. White, *E-mail@work.com: Employer Monitoring of Employee E-mail*, 48 ALA. L. REV. 1079, 1081 (1997).

166. Gantt, *supra* note 9, at 351–52; White, *supra* note 165, at 1081; S. REP. NO. 99-541, at 14 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568.

167. *See*, *e.g.*, Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457 (5th Cir. 1994). In *Steve Jackson Games, Inc.*, the Secret Service seized a computer belonging to the publishers that held private e-mail belonging to the publishers and 365 bulletin board system customers. The Fifth Circuit affirmed the district court's decision that this e-mail seizure violated the ECPA. *Id*. at 457–59, 464. *See also* Wesley College v. Pitts, 974 F. Supp. 375 (D. Del. 1997); Alexander I. Rodriguez, *All Bark, No Byte: Employee E-mail Privacy Rights in the Private-sector Workplace*, 47 EMORY L.J. 1439, 1449 (1998).

lawfulness.[168] Additionally, the Eleventh Circuit held in *Watkins v. L. M. Berry & Co.* that, under the ECPA, a personal call may be intercepted in the ordinary course of business only to the extent necessary to guard against unauthorized telephone use or to determine whether a call is personal. This demonstrates that the ECPA recognizes the principle of proportionality.[169] Finally, other federal and state laws may cover principles not implicitly recognized under the ECPA.[170]

The ECPA also provides both civil and criminal sanctions for violations. For example, the victim of an illegal interception may demand the greater of either $100 per day for each day on which a violation occurred, or $10,000 (plus punitive damages, reasonable attorney's fees, and other litigation costs reasonably incurred).[171] The victim of illegal access to an electronic storage system may demand at least $1,000 in damages, reasonable attorney's fees, and other litigation costs reasonably incurred.[172] Also, under the ECPA, a person who illegally intercepts an electronic communication may be imprisoned for a period of not more than five years.[173] A person who illegally accesses an electronic storage system may be imprisoned for up to two years.[174] Finally, fines for violations of the ECPA vary from $500 to $250,000.[175] Unlike Directive 95/46, however, the ECPA does not provide a right of access or a right to rectification.[176]

2. Three Exceptions under the ECPA

The ECPA provides some privacy protection. However, there are three exceptions to the ECPA's protection of the privacy of employee communication: prior consent, business use, and system provider.[177] These exceptions undermine the ECPA's protection of employee privacy.

---

168. 18 U.S.C. § 2511(1) (2000); 18 U.S.C. § 2701(a) (2000).
169. Watkins v. L. M. Berry & Co., 704 F.2d 577, 582–83 (11th Cir. 1983).
170. For example, federal legislation and some state statutes prohibit monitoring employees to monitor union activities. 29 U.S.C. § 158 (2000); 5 ILL. COMP. STAT. ANN. 315/10 (West 1986); CAL. GOV'T CODE § 12940 (West 1992); N.Y. LAB. LAW § 704 (McKinney 1983). This is related to the finality of the collection of data and the processing of sensitive data. *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION 363 (1996).
171. 18 U.S.C. § 2520(b), (c)(2) (2000).
172. 18 U.S.C. § 2707(b), (c) (2000).
173. 18 U.S.C. §§ 2511(4)(a), 2512(1) (2000).
174. 18 U.S.C. § 2701(b) (2000).
175. 18 U.S.C. §§ 2511(4), 2701(b) (2000).
176. *Cf.* Directive 95/46, *supra* note 11, arts. 12, 14.
177. White, *supra* note 165, at 1083.

a. The Prior Consent Exception

Interception by an employer of an employee's e-mail or other on-line communications, including stored electronic communications, is legal when the employee has expressly consented.[178] The ECPA permits the interception of an electronic communication when "one of the parties to the communication has given prior consent."[179] Similarly, an employer may access a stored electronic communication when "a user of that service with respect to a communication of or intended for that user" has given their authorization.[180]

The prior consent exception encompasses implied consent. In *Watkins v. L.M. Berry & Co.*, an employee sued her employer, claiming that her employer illegally intercepted a personal call.[181] The employer had an established policy (of which all employees were informed) of monitoring business calls.[182] Employees were permitted to make personal calls on company telephones,[183] and such calls, according to the policy, would only be monitored to the extent necessary to determine whether a particular call was of a personal or business nature.[184] While finding that consent must be specific and limited and generally should not be implied from the circumstances, the Eleventh Circuit nevertheless noted that limited implied consent was possible. It stated that courts could imply consent when an employee knew or should have known of an employee-monitoring policy, or when the employee placed personal calls on lines reserved for business communications that the employee knew were regularly monitored.[185]

In summary, while the consent exception places a limit on monitoring by employers,[186] employers may monitor employee communication as

178. *Id*. at 1083–84.
179. 18 U.S.C. § 2511(2)(d) (2000).
180. 18 U.S.C. § 2701(c)(2) (2000).
181. Watkins v. L.M. Berry & Co., 704 F.2d 577, 579 (11th Cir. 1983).
182. *Id.*
183. *Id.*
184. *Id*.
185. *Id*. at 581–82; Jeremy U. Blackowicz, *E-mail Disclosure to Third Parties in the Private-sector Workplace*, 7 B.U. J. SCI. & TECH. L. 80, 93 (2001) (explaining that the *Watkins* and *Deal* decisions, "while limiting the consent to specific circumstances, suggest that an employer with a monitoring policy in place may escape liability for intercepting e-mail messages"); Rodriguez, *supra* note 167, at 1460.
186. Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992). In *Deal*, the Spears owned a store that was robbed. Suspecting their employee Deal participated in the robbery, the Spears used a tape recorder to monitor business and personal phone calls made on the store phone. Without giving notice of the monitoring to Deal, the Spears recorded twenty-two hours of phone calls. Deal sued the Spears, and the district court found they had notated the ECPA. However, the Eighth Circuit refused to expand the consent exception through merely announcing the possibility of monitoring, finding this to be

long as they disclose a monitoring policy to their employees in advance and monitor the communications according to that policy.[187] This contrasts greatly with article 7(a) of Directive 95/46, which gives an employer in the private sector only limited justification for monitoring employee e-mail.[188]

b. The Business Use Exception

Employers can also monitor employee communication if the interception involves telephone equipment or facilities used within the ordinary course of business.[189] Although courts have never applied this exception directly to e-mail, courts have developed two approaches to interpreting this exception within the context of telephone monitoring.[190] These two approaches are the "context approach" and the "content approach."

Under the context approach, the court considers the circumstances in which an employer monitors an employee's communication. In *Deal v. Spears*, the Eighth Circuit articulated this approach as a two-pronged test.[191] The court required that the intercepting equipment: (1) be provided to the subscriber by the phone company or connected by the provider to the phone line; and (2) be used in the ordinary course of business.[192] Applying this test to e-mail monitoring in the workplace, the first prong is satisfied if an employer's computer connects to the Internet through a modem or network that uses a phone line.[193]

---

insufficient for a finding of employee consent to monitoring. *Id*. at 1157. *See also* Rodriguez, *supra* note 167, at 1460.

187. "Cases implicating the consent exception indicate that although an employer is at risk for liability if it engages in unrestrained monitoring, courts will usually rule in favor of an employer who has announced a monitoring policy to its employees and adhered to its limits. With respect to e-mail communications, the rulings in *Walonis* (Campiti v. Walonis, 611 F.2d 387 (1st Cir. 1979)), *Watkins*, and *Deal* bespeak the idea that such electronic communications could be accessed under the authority of a published monitoring policy. Consequently, a private employer who issues a policy to its employees is presumably only limited by the terms of the policy itself." Rodriguez, *supra* note 167, at 1460; Gantt, *supra* note 9, at 358 (pointing out that (1) with a comprehensive monitoring policy, "an employee's continued use of the e-mail network will presumably constitute, at a minimum, consent to employer interception of work-related messages and personal messages to the extent needed to determine whether the messages are personal or business in character," and (2) "[e]mployers can expand the permissible scope simply by offering legitimate interests justifying broad monitoring policies").

188. *See supra* Part II.B.1.

189. 18 U.S.C. § 2510(5)(a) (2000).

190. Blackowicz, *supra* note 185, at 91; Rodriguez, *supra* note 167, at 1453.

191. *Deal*, 980 F.2d at 1157.

192. *Id.*; *Rodriguez*, *supra* note 167, at 1455.

193. Blackowicz, *supra* note 185, at 91. The same logic likely applies if an employer's computer connects by ADSL (Asymmetric Digital Subscriber Line) or optic fiber. In these instances, a

To determine whether monitoring is within the ordinary course of business, thereby satisfying the second prong of the context approach, the court examines the circumstances surrounding the monitoring.[194] Central to this analysis is the court's consideration of: whether employees had notice that the employer might intercept communications; whether the employer has a legitimate business reason justifying the monitoring policy; and whether the time and scope of the monitoring were proportionate to the business reason.[195] Because legitimate interests in monitoring abound for employers—including security, the promotion of workplace efficiency, and the prevention of trade secret dissemination—advance notice will often justify e-mail monitoring by a private sector employer as long as the monitoring is proportionate.

However, when the extent of the monitoring exceeds the business interests, courts applying the context approach generally find the monitoring is not exempt from the ECPA. For example, while the Eighth Circuit recognized in *Deal* that the employer's interest in determining whether their employee participated in a robbery of the store was legitimate, it concluded that the recording of twenty-two hours of calls, regardless of their relation to his business interests, was excessive.[196] Because the extent of the monitoring was not justified by the legitimate business interest, the business use exception did not apply.[197]

Thus, these principles lead to the conclusion that: (1) monitoring professional e-mail of an employee by an employer does not pose a legal problem in the private-sector; and (2) monitoring personal e-mail to determine whether the employee is abusing the employer's equipment is allowed if the employer adopts a policy that limits or prohibits personal e-mail in the workplace.

Alternatively, under the content approach, courts focus on the subject matter of the communication.[198] Courts have ruled that employers may lawfully intercept all business communications, but that they have only a limited right to monitor personal communications.[199] For example, in *Watkins*, the court held an employer must show they intercepted an

---

telecommunication company provides ADSL or optic fiber to an employer and connects the monitoring equipment, which is installed in office computers belonging to the employer, to the ADSL or optic fiber. As a result, ADSL and optic fiber will also meet the first prong of the "context approach."

194. Rodriguez, *supra* note 167, at 1453.

195. *Deal*, 980 F.2d at 1158; Rodriguez, *supra* note 167, at 1454–45.

196. *Deal*, 980 F.2d at 1158.

197. *Id.*

198. Rodriguez, *supra* note 167, at 1456.

199. Gantt, *supra* note 9, at 367; Rodriguez, *supra* note 167, at 1456.

employee's communication in pursuit of a legal interest.[200] The court concluded that the monitoring of personal calls is permissible to the extent necessary to guard against unauthorized telephone use or to determine whether a call is personal.[201] Thus, the content approach does not completely eliminate the monitoring of an employee's personal e-mail in the private-sector workplace.[202]

c. The Provider Exception

The third exception to the ECPA is the provider exception, which lets system providers monitor employee e-mail.[203] This exception may potentially allow many employers to monitor employee communication. The central issue in these cases is whether an employer qualifies as a system provider. In *Flanagan v. Epson America*, a California court noted in a footnote that the provider exception would have exempted a private network provider from liability.[204] Given that an employer is often a private network provider (as the owner of a company's e-mail system), this exception will allow an employer to monitor freely employee e-mail.[205]

---

200. *Watkins*, 704 F.2d at 579; Blackowicz, *supra* note 185, at 92.

201. *Watkins*, 704 F.2d at 583.

202. *Cf.* Blackowicz, *supra* note 185, at 93.

203. Flanagan v. Epson America, Inc., No. BC 007036 (Cal. Super. Ct. Mar. 12, 1991), *cited in* Gantt, *supra* note 9, at 359. 18 U.S.C. § 2511 creates an exception for business-use interceptions:

> It shall not be unlawful under this chapter for 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, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

18 U.S.C. § 2511(2)(a)(i). § 2701(c)(1) creates an exception for stored communications when conduct is authorized "by the person or entity providing a wire or electronic communications service." 18 U.S.C. § 2701(c)(1) (2000).

A person or entity may divulge the contents of a communication to a person employed or authorized, or to a person whose facilities are used to forward such communication to its destination. Disclosure is also permitted when it is necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service. 18 U.S.C. § 2702(b)(4)–(5) (2000).

204. Gantt, *supra* note 9, at 359–60.

205. Blackowicz, *supra* note 185, at 90–91. *See also* Kevin P. Kopp, *Electronic Communications in the Workplace: E-mail Monitoring and the Right of Privacy*, 8 SETON HALL CONST. L.J. 861, 872–73 (1998) (suggesting that the provider exception will broadly exempt employer-providers). In *Bohach v. City of Reno*, one of the cases explained in Kopp's article, the internal affairs division of the Reno Police Department began an investigation of the messages several officers were sending over the computerized pager system. The officers sued the City of Reno for violating the ECPA and the Constitution. Finding that the ECPA's provider exception applied to the city, the district court

Overall, the three ECPA exceptions—the prior consent, the business use, and the provider exceptions—enable an employer in the private-sector to monitor employee e-mail by providing advance notice of the monitoring.[206] And, as such, these exceptions swallow the general protections provided by the ECPA.

C. State Law

While most state constitutions do not protect the privacy of a private person from infringement by another private person, most states do have statutes that regulate or restrict the interception of wire communications. Additionally, state common law has developed monitoring limits. Even given these restrictions on monitoring, it is difficult for an employee to establish their case under state statutes and common law.

1. State Constitutions and Statutory Law

Like the U.S. Constitution, the constitutions of most states neither explicitly nor implicitly protect a person's right to privacy from invasion by a private actor. The constitution of California provides some protection,[207] but to justify an invasion, an employer still would only need to show that the invasion substantially furthered a "competing" and "legitimate" countervailing interest.[208] Given an employer's aforementioned interests in security, efficiency, and the prevention of trade secret dissemination, employers will likely prevail under the California constitution.

Additionally, though most states have statutes to limit or regulate e-mail monitoring, they are usually insufficient to protect employee privacy.

---

analogized this pager system to e-mail. *See* Bohach v. City of Reno, 932 F. Supp. 1232, 1233–34, 1236 (D. Nev. 1996).

206. An employer probably ends up monitoring an employee's personal e-mail at least incidentally under the ECPA exceptions.

207. Rodriguez, *supra* note 167, at 1446–47. In California, the state constitutional protection applies to both public and private employers. Thus, no state action is necessary to make a constitutional claim against a private-sector employer. *See* DECKER, *infra* note 272, at 131.

208. Hill v. National Collegiate Athletic Ass'n, 865 P.2d 633 (Cal. 1994). Until *Hill*, California case law required employers show a compelling interest in order to justify their invasion of employee privacy. The court in *Hill*, however, distinguished invasions of interests "fundamental to personal autonomy" from invasions of "less central" privacy interests. To justify an invasion of an interest "fundamental to personal autonomy," an employer must demonstrate a compelling interest. Conversely, an employer need only present a countervailing interest to justify infringing a "less central" interest under *Hill*. The court then established a balancing test, which requires the privacy interests at issue "be specifically identified and carefully compared with *competing* or *countervailing* privacy and non-privacy interests." Gantt, *supra* note 9, at 391–92.

Theoretically, states may enact laws that protect the right to privacy to a greater extent than the ECPA because the ECPA typically only preempts state laws that are less protective than the federal law.[209] However, some state statutes fail to include electronic messages within the category of protected communications.[210] Moreover, because most are modeled on the ECPA,[211] state statutes have exceptions similar to those of the ECPA. Even though these exceptions may be narrower than those under the ECPA,[212] state statutes modeled on the ECPA nevertheless have similar weaknesses.

Connecticut and Delaware enacted statutes modeled on the Notice of Electronic Monitoring Act.[213] Under the Connecticut statute, an employer who engages in electronic monitoring must give prior written notice to employees[214] listing the possible types of monitoring.[215] The employer must post the notice in a conspicuous place that is readily accessible to employees.[216] Under the Delaware statute, an employer cannot monitor or otherwise intercept any telephone, e-mail, or internet transmission by an employee unless the employee has first been notified.[217] Such notice must be in writing and signed by the employee.[218]

These statutes have their limits. First, when an employer prohibits personal e-mail and gives employees advance notice of e-mail monitoring, these statutes may justify such monitoring on the basis of the employer's interest in checking for violations of the personal e-mail prohibition. Second, the Connecticut statute, for instance, allows an employer, under certain conditions, to engage in electronic monitoring without giving employees prior notice.[219]

---

209. *Id*. at 395.

210. Rodriguez, *supra* note 167, at 1461.

211. *Id*. at 1461 n.149.

212. Gantt, *supra* note 9, at 395; Rodriguez, *supra* note 167, at 1461. In general, courts interpret exceptions to state law more narrowly than exceptions to the ECPA. For example, unlike the ECPA, some states require the consent of all parties for monitoring to be legal. *See generally* Gantt, *supra* note 9, at 395–403.

213. Virginia General Assembly Joint Commission on Technology & Science, Privacy Advisory Committee, *Privacy Advisory Committee Summaries: Notice of Electronic Monitoring Act*, *at* http://jcots.state.va.us/Studies/Privacy/2001/2001_Summaries.htm (last visited Jan. 10, 2005).

214. CONN. GEN. STAT. § 31-48d(b)(1) (2001).

215. *Id.*

216. CONN. GEN. STAT. ANN. § 31-48d(b)(1) (2003).

217. DEL. CODE ANN. tit. 19, § 705(b) (2001).

218. *Id*.

219. Section 31-48d(b) of the Connecticut statute states:

> (2) When (A) an employer has reasonable grounds to believe that employees are engaged in conduct which (i) violates the law, (ii) violates the legal rights of the employer or the employer's employees, or (iii) creates a hostile workplace environment, and (B) electronic

2. State Common Law

State common law provides four invasion of privacy causes of action: (1) unreasonable intrusion on the seclusion of another; (2) misappropriation of another's name or likeness; (3) unreasonable publicity given to another's private life; and (4) publicity that unreasonably places another in a false light before the public.[220] Of these, the cause of action for unreasonable intrusion on the seclusion of another usually applies to employee communication privacy cases.[221]

The Fourth Amendment balancing test influences courts assessing causes of action dealing with an unreasonable intrusion on the privacy of another.[222] This balancing test compares an individual's expectation of privacy with the interests of the government in engaging in the conduct at issue.[223] Courts employ a similar balancing test when they examine an invasion of privacy cause of action. Such an action typically has four elements.[224] First, the intrusion must have been intentional.[225] Second, the act must be highly offensive to the reasonable person.[226] Third, the plaintiff's activity must have been subjectively and objectively private.[227] Fourth, the intruder cannot have had a legitimate purpose justifying the

---

monitoring may produce evidence of this misconduct, the employer may conduct monitoring without giving prior written notice.

CONN. GEN. STAT § 31-48d (b)(2) (2001).

220. *See* RESTATEMENT (SECOND) OF TORTS §§ 652B-E (1976); Cantrell v. American Broadcasting Cos., 529 F. Supp. 746, 756 (N.D. Ill. 1981) (stating that Illinois recognizes all four causes of action for invasion of privacy); Ward v. Connor, 495 F. Supp. 434, 439 (E.D. Va. 1980) (stating that a number of jurisdictions recognize all four invasion of privacy causes of action); Sanchez-Scott v. Alza Pharmaceuticals, 86 Cal. App. 4th 365, 372 (2001) (stating that California recognizes all four invasion of privacy causes of action).

221. Rodriguez, *supra* note 167, at 1462.

222. Gantt, *supra* note 9, at 380; Rodriguez, *supra* note 167, at 1443.

223. Katz v. United States, 389 U.S. 347 (1967). Justice Harlan's concurring opinion in *Katz* has influenced the analysts of other courts in Fourth Amendment cases. Justice Harlan suggested that an individual has a constitutionally-recognized expectation of privacy when they satisfy a two-prong test. First, the individual must have exhibited an actual, subjective expectation of privacy. Second, society must be prepared to recognize that expectation as "reasonable." *Id*. at 361 (Harlan, J., concurring). *See also* Rodriguez, *supra* note 167, at 1443 n.25 (citing Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349 (1974)); O'Connor v. Ortega, 480 U.S. 709 (1987) (taking a balancing approach).

224. Rodriguez, *supra* note 167, at 1463.

225. *See, e.g.*, Benn v. Florida E. Coast Ry. Co., 1999 U.S. Dist. LEXIS 14314, at *22–23 (S.D. Fla. 1999); Patton v. United Parcel Serv., 910 F. Supp. 1250, 1276 (S.D. Tex. 1995); Winegard v. Larsen, 260 N.W.2d 816, 822 (Iowa 1977).

226. *See, e.g.*, Borse v. Piece Goods Shop, Inc., 963 F.2d 611, 622 (3d Cir. 1992); Keating v. Bucks County Water & Sewer Auth., 2000 U.S. Dist. LEXIS 18690, at *44 (E.D. Pa. 2000); Farrington v. Sysco Food Servs., 865 S.W.2d 247, 253 (Tex. Ct. App. 1993).

227. Rodriguez, *supra* note 167, at 1463 n.168.

invasion.[228] This balancing test, which examines the reasonableness of the privacy expectation, parallels the approach used in *Halford v. United Kingdom*.[229]

When these elements are applied to actual facts, however, it is difficult for an employee to establish their case.[230] For example, a court may find that the act in question is not highly offensive to the reasonable person because of the gradual nature of the monitoring[231] or because the employer gave notice of the monitoring.[232] Courts may also be reluctant to find that an employee's work environment is sufficiently private for an invasion to occur.[233] Thus, courts tend to conclude that an employers' interest prevails over employees' privacy interest.[234]

For example, in *Smyth v. Pillsbury Corp*., an employee sued his employer for a common law invasion of privacy.[235] The employee alleged that the employer intercepted the employee's e-mail, even though the employer had repeatedly assured employees that e-mail communications were confidential and privileged.[236] The court concluded that the employer's interest in preventing inappropriate and unprofessional comments or illegal activity from occurring over its e-mail system outweighed any privacy interest the employee may have had in her e-mail.[237] This case illustrates that, in sum, employers are likely to prevail under state common law.[238]

Overall, in the United States, a private-sector employer is likely able to monitor both the professional and personal e-mail of their employees so long as they provide employees with advance notice of the monitoring. Because U.S. statutes and common law do not distinguish business from non-business hours, this distinction is largely ignored in the United

228. Courts often describe this element as whether the information publicized is not of legitimate concern to the public. *See, e.g.*, Johnson v. Sawyer, 47 F.3d 716, 731 (5th Cir. 1995); Faison v. Parker, 823 F. Supp. 1198, 1205 (E.D. Pa. 1993).

229. *See supra* Part II.C.

230. Wilborn, *supra* note 9, at 844.

231. *Id*. This standard frequently forecloses an employee's claim based on typical workplace monitoring and surveillance. Routine monitoring can appear harmless from some perspectives, especially that of a third party, and the negative effects of such monitoring are often gradual and incremental. *Id.*

232. Rodriguez, *supra* note 167, at 1463–64. For example, if an employer notified employees that e-mail monitoring could occur, a court may conclude that the employer's acts were not highly offensive and that an objective expectation of privacy was unreasonable at the time. *Id.*

233. Wilborn, *supra* note 9, at 846.

234. White, *supra* note 165, at 1097.

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

236. *Id*. at 98.

237. *Id*. at 101; White, *supra* note 165, at 1098.

238. Rodriguez, *supra* note 167, at 1464; Wilborn, *supra* note 9, at 846.

States.[239] If this distinction is ignored, the legal treatment of private-sector e-mail monitoring in the workplace in the United States will likely be very similar to that in Western Europe.

IV. DATA PROTECTION OF PRIVATE-SECTOR EMPLOYEES IN WESTERN EUROPE AND THE UNITED STATES

The preceding parts of this Article have shown that Western Europe and the United States provide similar levels of data protection for private-sector employees. In both regions, a private-sector employer may monitor employee e-mail with advance notice of monitoring; however, the level of monitoring allowed will not necessarily remain similar in Western Europe and the United States. The right to privacy enjoys a higher status in Western Europe than it does in the United States, and the government plays a greater role in its protection in Western Europe. In light of a recent French case and a series of corporate scandals in the United States, it is likely that Western Europe will increase data protection accorded private-sector employees to a greater extent than the United States.

A. Factors to Consider in Predicting the Future: The Status of the Right to Privacy and the Role of Government

To increase the level of private-sector employee data protection, new statutes or an evolution in the treatment of the principle in case law will be necessary. This, however, depends on the status of the right to privacy and the role of government. The more protected the right to privacy, the more likely statutes or case law will change. Similarly, the larger the role of the government, the more likely there will be governmental action that will increase the level of data protection for employees. The right to privacy enjoys a higher status and the government plays a greater role in protecting citizens in Western Europe than in the United States. Thus, data protection is likely to be advanced to a greater extent in Western Europe.

1. The Status of the Right to Privacy

a. In Western Europe

In Western Europe, important texts at both the supranational and national levels establish the right to privacy as a fundamental right. For

239. *Id.*

example, the 1950 European Convention of Human Rights (ECHR) specifically provides in article 8 for the right to privacy.[240] All twenty-five member states of the European Union are parties to the ECHR,[241] and, therefore, recognize the right to privacy. Article 7 of the Charter of Fundamental Rights of the European Union[242] also designates the right to privacy as fundamental.[243] In addition to these supranational texts, laws at the national level also guarantee the right to privacy. For example, Germany's Basic Law protects the right to privacy by guaranteeing human dignity[244] and the freedom of personality.[245] Similarly, the Spanish Constitution has a specific provision on the right to privacy.[246]

Moreover, Western Europe specifically guarantees data protection as a fundamental right. Article I of the Council of Europe Convention explicitly includes data protection within the fundamental right to

240. Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, art. 8, 313 U.N.T.S. 222, *available at* http://conventions.coe.int/Treaty/EN/Treaties/Html/005.htm (last visited Nov. 17, 2004) [hereinafter ECHR]. Article 8 of the ECHR provides:

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

Id.

241. The twenty-five Member States of the European Union are Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Maltar, the Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom. *See* European Union, *European Union Member States*, *at* http://www.europa.eu.int/abc/government/index_en.htm (last visited Nov. 16, 2004). Austria, Belgium, Denmark, Germany, Ireland, Italy, Luxembourg, the Netherlands, Sweden and the United Kingdom ratified the ECHR in the 1950s. The other Member States had all ratified by 1998. *See* Council of Europe, Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms, *at* http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=005&CM=8&DF=1/24/05&CL=ENG (last visited Jan. 10, 2005).

242. Charter of Fundamental Human Rights of the European Union, 2000 O.J. (C 364/01), [hereinafter Charter]. The president of the European Parliament, the Council and the Commission signed the Charter at the European Council meeting in Nice on December 7 to 9, 2000. For the first time in the European Union's history, the Charter enumerates in a single text the entire range of civil, political, economic, and social rights of European Union citizens and residents. The Charter confirms human rights recognized by various legal instruments, including the ECHR and the constitutions of member states of the European Union. *See* European Parliament, *The Charter of Fundamental Human Rights of the European Union*, *available at* http://www.europarl.eu.int/charter/default_en.htm (last visited Nov. 17, 2004).

243. Charter, *supra* note 242, art. 7; ECHR, *supra* note 240, art. 8.

244. Art. 1, para. 1 GG.

245. Art. 2, para. 1 GG. *See also* Monahan, *supra* note 54, at 283.

246. CONSTITUĆION ESPAÑOLA [SPANISH CONSTITUTION] [C.E.] art. 18, para. 1. *See also* Monahan, *supra* note 54, at 283.

privacy.[247] Directive 95/46 also considers data protection to be a fundamental privacy right.[248] Furthermore, the European Union Charter of Fundamental Rights provides for data protection.[249] At the national level, the Spanish constitution includes a specific provision placing electronically stored data within its iteration of the right to privacy.[250]

In addition, Western Europe recognizes these fundamental privacy rights in the workplace. The European Court of Human Rights took this position in *Niemietz v. Germany*.[251] In *Niemietz*, an anti-clerical activist wrote a letter threatening a judge who was presiding over the criminal proceeding of a person who had failed to pay their Church tax.[252] The letter came from a branch of a political party called *Freiburg Bunte Liste*.[253] Because Niemietz, another anti-clerical activist, had previously chaired *Freiburg Bunte Liste*, letters addressed to the political party were forwarded to his office[254] and the Munich District Court issued a search warrant for Niemietz's office.[255] Niemietz argued that the search violated his right to privacy under article 8 of the ECHR,[256] while Germany contended that article 8 does not protect professional life.[257]

Rejecting the distinction between private and professional contexts, the European Court of Human Rights declared that:

> Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings.
>
> There appears, furthermore, to be no reason of principle why this understanding of the notion of "private life" should be taken to

247. Council of Europe Convention, *supra* note 30, art. 1.

248. Directive 95/46, *supra* note 11, art. 1, para. 1.

249. Charter, *supra* note 242, art. 8. Article 8 provides:

> 1. Everyone has the right to the protection of personal data on themselves.
>
> 2. Such data must be fairly processed for specified purposes with either the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right to access and rectify data collected concerning themselves.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

Id.

250. CONSTITUĆION ESPAÑOLA, *supra* note 246, art. 18, para. 4.

251. Niemietz v. Germany, 251-B Eur. Ct. H.R. 23 (1992), *available at* http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=niemetz%20%7C%20v.%20%7C%20germany&sessionid=563786&skin=hudoc-en (last visited Dec. 20, 2004).

252. *Id*. at 27.

253. *Id.*

254. *Id*.

255. *Id*. at 32.

256. *Id*. at 33.

257. *Id*.

> exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world. This view is supported by the fact that, as was rightly pointed out by the Commission, it is not always possible to distinguish clearly which of an individual's activities form part of his professional or business life and which do not.[258]

Thus, in *Niemietz*, the European Court of Human Rights held that the fundamental right to privacy extends to the workplace. The European Court of Human Rights later affirmed this position in *Amann v. Switzerland*.[259]

At the national level, Belgium protects an employee's right to privacy in the workplace by emphasizing human dignity. The Belgian Privacy Commission, an independent organ of the Belgian government responsible for the regulation of personal data processing and the protection of privacy,[260] declared that making employees work under constant surveillance contravenes human dignity and is not necessarily productive.[261] Accordingly, the Commission concluded that an employer cannot monitor all aspects of employee activities.[262]

The law in Finland is in agreement with the stance of the Belgian Commission. In October 2001, Finland's Act on the Protection of Privacy in Working Life entered into force.[263] The purpose of the act is "to implement the protection of private life and other basic rights safeguarding privacy, and to promote the development of and compliance with good processing practice, when personal data are processed in working life."[264]

---

258. *Id.*

259. Amann v. Switzerland (27798/95), [2000] Eur. Ct. H.R. 87 (2000), *available at* http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=amann%20%7C%20v.%20%7C%20switzerland&sessionid=563797&skin=hudoc-en (last visited Jan. 18, 2005).

260. *Commission de la Protection de la Vie Privée* [Belgian Privacy Commission], *Plan de Gestion* [Strategic Development Plan] ver. 12, Oct. 15, 2003, *available at* http://www.privacy.fgov.be/la_commission/plan_de_gestion.pdf (last visited Nov. 17, 2004).

261. *Commission de la Protection de la Vie Privée* [Belgian Privacy Commission], *Avis de initiative relatif à la Surveillance par l'Employeur de l'Utilisation du Système Informatique sur le Lieu de Travail* [*Opinion on Employer Monitoring of Computer System Usage in the Workplace*] (Apr. 3, 2000), *available at* http://193.191.208.6/juris/jurfv.htm (last visited Nov. 17, 2004). *See also* JEAN-EMMANUEL RAY, LE DROIT DU TRAVAIL À L'EPREUVE DES NTIC [LABOR LAW FACING THE TEST OF NEW TECHNOLOGY OF THE INFORMATION AND COMMUNICATION] 102–04 (2d ed. 2001).

262. *Id.*

263. The Act on Protection of Privacy in Working Life (477/2001), Oct. 1, 2001 (Finland), *available at* http://www.mol.fi/english/working/dataprotection.html (last visited Nov. 17, 2004).

264. *Id.* art. 1.

Applicable to both the private and public sector,[265] article 9 states that "employer actions shall not jeopardize the secrecy of the employee's private, confidential messages when using electronic mail or data networks."[266]

Overall, Europe considers the right to privacy, including data protection, to be fundamental, even in the workplace. It seems likely that England will give the right to privacy similar treatment. Admittedly, England shares with the United States the common law tradition, which does not necessarily regard the right to privacy as fundamental. Indeed, the Lawful Business Practice Regulation of 2000, a British regulation of telecommunication monitoring in business, broadly allows an employer in the private-sector to monitor employee e-mail.[267] However, the case law of the European Court of Human Rights is binding authority in the United Kingdom because it is a party to the treaty establishing the court. The United Kingdom is also a member of the European Union, which, as mentioned, considers the right to privacy as fundamental. As a result, the United Kingdom will be constrained to respect the right to privacy. Indeed, some judgments in the United Kingdom already cite article 8 of the ECHR as an important source for the right to privacy.[268]

b. The United States

A citizen has the right to privacy under the constitutional scheme of the United States.[269] As early as the late nineteenth century, the Supreme Court of the United States recognized that the Fourth and Fifth Amendments protect an individual's home and privacy.[270] In *Mapp v. Ohio*, the Court recognized that the right to privacy is an important right reserved to the people.[271] Then, in *Griswold v. Connecticut*, the Court

265. *Id.* art. 2.

266. *Id.* art. 9, para. 4.

267. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations, (2000) SI 2000/2699, *available at* http://www.hmso.gov.uk/si/si2000/20002699.htm (last visited Nov. 17, 2004). Because this regulation allows an employer to monitor any telecommunication to determine whether it relates to business (*Id*. art. 3(2)(a)), it is similar to the ECPA business exception.

268. *See*, *e.g.*, Campbell v. MGN Ltd., [2004] E.M.L.R. 15, *available at* 2004 WL 852411; Douglas v. Hello! Ltd., [2004] E.M.L.R. 14, para. 16, *available at* 2004 WL 62050.

269. Rodriguez, *supra* note 167, at 1442–43; Martha Rundell, *Decisions Between Consenting Adults Made in Private—No Place for the Government to Tread*, 60 LA. L. REV. 877, 878 (2000).

270. Boyd v. United States, 116 U.S. 616 (1886). The court explained that the doctrines underlying the Fourth and Fifth Amendments "apply to all invasions on the part of the government and its employes of the sanctity of a man's home and the privacies of life." *Id*. at 630.

271. Mapp v. Ohio, 367 U.S. 643 (1961). In *Mapp*, the Court applied the exclusionary rule, which

concluded that emanations from various guarantees in the Bill of Rights create a zone of privacy.[272] Thus, the U.S. Constitution guarantees the right to privacy indirectly through several amendments, rather than directly through a single amendment.

However, the absence of a specific amendment protecting the right to privacy leaves the right vulnerable, because it allows other rights, especially those explicitly guaranteed by the Constitution, to compete with privacy interests.[273] For example, courts often protect First Amendment rights in the face of conflict with the right to privacy, as evidenced by the rarity with which courts enjoin the dissemination of information based on the invasion of privacy. Most states share this problem, as only ten state constitutions explicitly guarantee the right to privacy.[274]

In *Planned Parenthood of Columbia/Willamette, Inc. v. American Coalition of Life Activists*, the Ninth Circuit addressed the question of injunctive and monetary relief against persons and organizations publishing photographs, addresses, and other personal information about

---

requires a Court to exclude evidence obtained through an unlawful search or seizure from a criminal trial, to evidence collected by state police officers. The Court noted that if it adopted another rule, "the right to privacy, no less important than any other right carefully and particularly reserved to the people would stand in marked contrast to all other rights declared as 'basic to a free society.'" *Id*. at 656.

272. Griswold v. Connecticut, 381 U.S. 479, 484 (1965). The Court held that emanations from the First, Third, Fourth, Fifth, and Ninth form the basis of the right of privacy. *See* Charlesworth, *supra* note 13, at 91 (stating that the First, Third, Ninth, and Fourteenth Amendments are relevant to the right to privacy in addition to the Fourth and Fifth Amendments); KURT H. DECKER, EMPLOYEE PRIVACY LAW AND PRACTICE 107 (1987) (noting that the First, Fourth, Fifth, Ninth, and Fourteenth Amendments relate to the right to privacy).

273. CATE, PRIVACY IN THE INFORMATION AGE, *supra* note 19, at 100.

274. These ten states are Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington. *See* ALASKA CONST. art. I, § 22 ("The right of the people to privacy is recognized and shall not be infringed."); ARIZ. CONST. art. II, § 8 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law."); CAL. CONST. art. 1, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."); FLA. CONST. art. I, § 23 ("Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein."); HAW. CONST. art. I, § 6 ("The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest. The legislature shall take affirmative steps to implement this right."); ILL. CONST. art. I, § 6 ("The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications by eavesdropping devices or other means."); LA. CONST. art. I, § 5 ("Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy."); MONT. CONST. art. II, § 10 ("The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest."); S.C. CONST. art. I, 10 ("The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and unreasonable invasions of privacy shall not be violated . . ."); WASH. CONST. art. I, § 7 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law.").

doctors and other abortion service providers on an anti-abortion website called the "Nuremberg Files."[275] While the court declined to decide whether the First Amendment would protect defendants in an invasion of privacy suit,[276] the Ninth Circuit reversed the district court decision, which enjoined the dissemination of addresses and other personal information on doctors and others.[277] Even though it admitted that the website frightened doctors and included offensive statements, the court nevertheless allowed the dissemination of such personal information.[278]

In *City of Kirkland v. Sheehan*, an unreported case from Washington State, the King County Superior Court dealt with a similar issue.[279] Plaintiffs sought to enjoin the operation of a website that was critical of law enforcement officers and listed the names, addresses, birth dates, telephone numbers, and social security numbers of the officers, as well as other personal information.[280] The court concluded that this dissemination of legally obtained private addresses, telephone numbers, and other personal information is speech protected by the First Amendment. The court enjoined the dissemination of the social security numbers, however, because access to an individual's social security number enables a third party to control, manipulate, or alter other personal information.[281]

The status of the right to privacy in the workplace is less elevated in the United States than in Western Europe. Of the amendments supporting a zone of privacy, the Fourth Amendment, which prohibits unreasonable searches and seizures, forms the core. The Fourth Amendment's protection of privacy began with the prohibition of unreasonable searches and seizures in the home.[282] Additionally, in an influential article on the right to privacy, Samuel Warren and Louis Brandeis argued that the right to privacy forbids invasion by a private person in domestic life.[283] These principles lead to the conclusion that an employer must respect employee privacy outside the office and at home. On the other hand, the right to privacy has developed with a distinction between professional and personal space.[284] While the right protects personal space, courts generally

275. Planned Parenthood of Columbia/Willamette, Inc. v. American Coalition of Life Activists, 244 F.3d 1007 (9th Cir. 2001).
276. *Id*. at 1016 n.10.
277. *Id*. at 1020.
278. *Id*. at 1017.
279. City of Kirkland v. Sheehan, 29 Media L. Rep. 2367 (Wash. Super. May 10, 2001).
280. *Id*. at 2368.
281. *Id.* at 2372.
282. Boyd v. United States, 116 U.S. 616, 629–30 (1885).
283. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV 193 (1890).
284. *See supra* Part III.

do not apply it to professional spaces.[285] This distinction does not exist in Western Europe, where the right to privacy is considered fundamental even in the workplace.[286]

2. Role of the Government

In Western Europe, the government is expected to and does actively protect its citizens. Many Western European governments "provide, pay for and heavily regulate essential services."[287] For example, Western European governments generally maintain extensive social security systems intended to reduce social inequality.[288] "In fact, even in England, which has a common law tradition, the government often provides, or at least subsidizes many essential services, including education, housing and health care."[289] Viewing the government as a guarantor of their rights, European citizens accept and often appreciate the government's intensive involvement in their daily lives.[290]

Conversely, in the United States, the government does not play an active role in guaranteeing citizens' rights. American society is traditionally skeptical of government,[291] making it hard for the government to become involved in daily life to protect citizens' rights. Because of this skepticism, the government tends to play a role in protecting citizens'

---

285. *Id.*

286. *See supra* Part II.

287. CATE, PRIVACY IN THE INFORMATION AGE, *supra* note 19, at 44.

288. Carol Graham, *Public Attitudes Matter: A Conceptual Framework for Accounting for Political Economy in Safety Nets and Social Assistance Policies*, Dec. 2002, http://wbln0018.worldbank.org/HDNet/hddocs.nsf/0/8a423b475eb64f9c85256c9b005f9798/$FILE/0233.pdf (last visited Nov. 17, 2004).

289. CATE, PRIVACY IN THE INFORMATION AGE, *supra* note 19, at 44.

290. *Id*.

291. Fred H. Cate, *Privacy and Telecommunications*, 33 WAKE FOREST L. REV. 1, 33 (1998). Jane E. Kirtley explains:

> Privacy advocates urge the adoption of the European model for data protection in the name of protecting individual civil liberties. But in so doing, they ignore, or repudiate, an important aspect of the American democratic tradition: distrust of powerful central government. The Bill of Rights is supposed to protect the American people from the government. Statutes such as the federal Privacy Act and the Paperwork Reduction Act demonstrate that when it comes to privacy, Americans generally do not assume that the government necessarily has citizens' best interests at heart. This is especially so when the government piously invokes "protection of privacy" as the justification for withholding information, or perhaps even more significantly, for engaging in intrusive activities. The European paradigm assumes a much higher comfort level with a far more authoritarian government. Skeptical Americans want checks in the system to keep the government "honest."

Jane E. Kirtley, *The EU Data Protection Directive and the First Amendment: Why a "Press Exemption" Won't Work*, 80 IOWA L. REV. 639, 648–49 (1995).

rights only when there is a huge outcry from the public. Even then, the government's role tends to be modest, and its approach minimalist.

For example, Congress adopted the 1988 Video Privacy Protection Act after a journalist outraged the public by publishing a list of 146 videocassettes rented by a U.S. Supreme Court Justice candidate and his wife.[292] The Video Privacy Protection Act imposes civil liability on video service providers who disclose a customer's video rental record without the customer's authorization.[293] However, under this act, providers may release mailing lists, including a list of their customers' preferences by category, for direct marketing purposes.[294]

Similarly, Congress adopted the Driver's Privacy Protection Act[295] following a strong public reaction to an actress's murder by a fan. The fan obtained the actress's address from a detective who had learned it from the California Department of Motor Vehicles.[296] The Driver's Privacy Protection Act forbids a state's department of motor vehicles from releasing personal information from a driver's records,[297] though the act also allows fourteen exemptions to this prohibition.[298]

Overall, the United States regulates privacy on a category by category basis, while establishing exemptions to a regulation's restrictions. While the U.S. government is less active than governments in Western Europe in protecting citizens' rights, employer-employee relations play a supplemental role.[299] For example, collective bargaining agreements may potentially restrict permissible monitoring purposes.[300] However, because many employers monitor employee e-mail without advance notice to employees,[301] the effectiveness of company policy in protecting employee privacy may be limited.

B. The Future of Employee Data Protection in the Private-Sector After Nikon France *and U.S. Corporate Scandals*

Two recent events may potentially increase the level of data protection of private-sector employees. First, in October 2001, the French Court of

292. 18 U.S.C. § 2710 (2000). *See also* Charlesworth, *supra* note 13, at 93.
293. 18 U.S.C. § 2710 (b)(1)(2000).
294. Monahan, *supra* note 54, at 281.
295. Driver's Privacy Protection Act, 18 U.S.C. § 2721–2725 (2000).
296. Charlesworth, *supra* note 13, at 93
297. Driver's Privacy Protection Act § 2721(a); *see also* Charlesworth, *supra* note 13, at 93.
298. Driver's Privacy Protection Act § 2721(a); Charlesworth, *supra* note 13, at 93.
299. *Cf.* SCHWARTZ & REIDENBERG, *supra* note 170, at 367–77.
300. *Id*. at 369–70.
301. *Id*. at 375.

Cassation rendered a judgment in favor of an employee whose employer had accessed documents on the employee's office computer.[302] Second, in the United States, a series of corporate scandals, involving companies such as Enron and WorldCom, has increased distrust of employers. Taking into account the aforementioned factors, Western Europe will probably increase the level of data protection, while the United States most likely will not.

1. Nikon France

Nikon France v. Onof is an innovative judgment from the Court of Cassation.[303] Before *Nikon France*, the Court of Cassation had established two limits on monitoring by a private-sector employer. Even with these limits, however, an employer could monitor e-mail sent during business hours by providing advance notice to employees. *Nikon France* severely limited an employer's ability to monitor e-mail, even during business hours.

The Court of Cassation established these limits in *Néocel v. Spaeter*. In *Néocel v. Spaeter*, an employer fired a sales clerk after observing her through a hidden camera located near where she worked.[304] Holding that the images recorded by the camera were not admissible into evidence, the Court of Cassation reversed the judgment of the Court of Appeals in Colmar for the employer.[305]

First, the Court of Cassation declared that an employer in the private-sector must give employees advance notice of monitoring.[306] Second, it implied that an employer in the private-sector cannot monitor an employee during non-business hours. The Court of Cassation held, "[i]f the employer has a right to control and monitor the activity of her employees *during the business hours*, all the records, whatever the motive may be, of images or spoken words made without the employees' knowledge, constitute illegal mode of proof."[307] Because subordination to an employer's control mostly covers business hours, an employer has less

302. Cass. soc., Oct. 2, 2001, Bull Civ. V, No. 291.
303. *Id.*
304. Cass. soc., Nov. 21, 1991, Bull Civ. V, No. 519.
305. *Id*. *See also* MARIE-PIERRE FENOLL-TROUSSEAU & GERARD HAAS, LA CYBERSURVEILLANCE DANS L'ENTREPRISE ET LE DROIT [THE CYBERSURVEILLANCE IN THE COMPANY AND THE LAW] 29 (2002); Philippe Waquet, *Un Employer Peut-Il Filmer à Leur Insu Ses Salariés?* [*Can an Employer Film Her Employees without Their Knowledge?*], 1992 DR. SOC. 28, 31 (1992) [hereinafter Waquet I].
306. Cass. soc., Nov. 21, 1991, Bull Civ. V, No. 519.
307. *Id.* (emphasis added).

authority to control employees during non-business hours. This limit does not exist in either the case law of the ECHR or the European Court of Justice. The American system also does not have this limit.

While later judgments and the French Labor Code follow the prohibition of monitoring without notice established by *Néocel*,[308] French case law before *Nikon France* found few problems with the monitoring of employees in the private-sector during business hours, as long as the employer gave advance notice of the monitoring. For example, in March 2000, the Court of Cassation affirmed an employer's right to monitor the activity of employees during business hours.[309] The court concluded that an employer could listen to an employee's personal conversation on the employer's phone because the employer had given advance notice of the monitoring. In September 2000, *le Conseil de prud'hommes* in Montbéliard, a conciliation board for labor issues, upheld a sanction against an employee who sent personal e-mail during business hours.[310] In this case, a current employee sent a former employee information regarding the employer's reorganization plans despite the employer's prohibition on personal e-mail in the workplace.[311] In February 2000, *le Conseil de prud'hommes* in Paris similarly justified a sanction against an employee who sent an e-mail to a friend in Australia during business hours even though the employer had limited e-mail use to professional purposes.[312] Such sanctions are legitimate only if an employer can present evidence that an employee sent a personal e-mail. An employer often obtains this evidence, however, by monitoring employees. Thus, the logic of the October 2001 judgment of the Court of Cassation[313] applies to e-mail monitoring.

However, a subtle change in the notion of privacy created tension in France. In 1997, the Court of Cassation started to use the term, "*la vie personelle*," to designate the notion of privacy instead of "*la vie privée*,"

308. *See* Cass. soc., Dec. 10, 1997, Bull. Civ. V, No. 434 (surveillance by video camera); Cass. soc., Feb. 4, 1998, Bull. Civ. V, No. 64; Cass. soc., May 22, 1995, Bull. Civ. V, No. 164 (surveillance by a private detective); Cass. soc., May 15, 2001, RJS 7/01 No. 830 (monitoring the use of a vending machine by employees). *See also* C. TRAV., art. L. 121-8 (Fr.).

309. Cass. soc. Mar. 14, 2000, Bull. Civ. V, No. 101.

310. C.P.H. Montbéliard, Sept. 19, 2000, RG No. F 00/00022.

311. *Id.*; Note, 1042 SEM. SOC. LAMY 13 (2001).

312. C.P.H. Paris, Feb. 1, 2000, No. 99-08.523. While the Court of Appeals in Paris also justified a sanction in a similar situation, C. Paris, May 22, 2000, RG No. 298/34330, *le Conseil de prud'hommes in Nanterre* did not uphold a sanction against an employee who accessed a pornographic website during business hours. However, in that case, it was easy to manipulate the data on the sites visited by the employee stored on the hard drive. C.P.H. Nanterre, July 16, 1999, RG No. F 98/013.

313. *See supra* note 301.

which had been used previously.[314] The former notion is broader than the latter and assumes that privacy exists, even during business hours, both in and outside the workplace.[315] This new notion of privacy, however, conflicted with established law, which allowed an employer in the private-sector to monitor an employee's professional and personal e-mail as long as there was advance notice. The judgment in *Nikon France* came in the middle of this tension.

In *Nikon France*, the Court of Cassation declared that an employer cannot read personal messages sent or received by an employee on a computer belonging to their employer and used by the employee for their work.[316] Nikon France, the employer of Frédéric Onof, opened and copied two folders titled "personal" and "fax," respectively, from Onof's computer while he was absent.[317] Examining those folders, the employer found that Onof had used the computer for personal activities despite the employer's prohibition on such use.[318]

In condemning the actions of Nikon France, the Court of Cassation stated that an employee has a right to respect for their privacy, even during business hours and in the workplace.[319] The Court of Cassation declared that it would be a violation of a fundamental freedom, namely the right to privacy and secrecy of correspondence, for an employer to read personal messages sent or received by their employee on a computer belonging to the employer and used by the employee for work.[320] The Court of Cassation added that monitoring personal messages violates this fundamental freedom even if the employer prohibits the usage of the computer for non-professional purposes.[321] As a result, the state of the law in France is now that, absent exceptional circumstances, an employer in the private-sector cannot monitor personal e-mail sent by an employee during business hours, even if the employer has given advance notice of the monitoring or has prohibited the use of e-mail for personal purposes.[322]

In *Nikon France*, the Court of Cassation furthered the notion of "*la vie personnelle*" by recognizing that an employee has a right to privacy in the

---

314. Philippe Waquet, *Retour sur l'arrêt Nikon* [*Return to the Nikon Judgment*], 1065 SEM. SOC. LAMY 5, 6 (2002) [hereinafter Waquet II].

315. *Id.*

316. Cass. soc., Oct. 2, 2001, Bull Civ. V, No. 291.

317. Stanislas Kehrig, *Disque Dur de l'Employeur et Vie Personnelle du Salarié* [*Hard Disk of the Employer and Privacy of the Employee*], 1045 SEM. SOC. LAMY 6, 6 (2001).

318. *Id.*

319. Cass. soc., Oct. 2, 2001, Bull Civ. V, No. 291.

320. *Id.*

321. *Id.*

322. Kehrig, *supra* note 317, at 9.

workplace during business hours. The Court of Cassation relied on article 8 of the ECHR,[323] article 9 of the French Civil Code,[324] article 9 of the New French Code of Civil Procedure,[325] and article L. 120-2 of the French Labor Code.[326] However, it did not cite Directive 95/46 in coming to its decision.

Article 9 of the New French Code of Civil Procedure addresses fairness of proof in two senses. The notion of fairness is respected through its prohibition on monitoring without advance notice, which has been an integral part of French case law since *Néocel*. Additionally, the case law since *Nikon France* seems to show that fairness of proof requires the presence of the employee when monitored by the employer. In December 2001, the Court of Cassation concluded that it was illegal for an employer to fire an employee after opening the employee's personal closet during his absence and finding cans of beer.[327] According to the court, a company's internal regulations must set forth the conditions under which monitoring would be undertaken,[328] and the presence of the employee at the time of monitoring is mandatory.[329] *Nikon France* mentioned article 9 of the New French Code of Civil Procedure. This, taken in conjunction with the facts of the case (the employee was absent during the monitoring by Nikon France and whether there was advance notice of monitoring was unclear) and the fact that case law began to explicitly require the presence of the employee only after *Nikon France*, makes it likely that the employee's absence was a factor in finding a violation of article 9 of the New French Code of Civil Procedure.

The court's citation of article L. 120-2 of the French Labor Code shows that the principle set forth in *Nikon France* is itself not innovative. Attempting to balance the interests of employers and employees, article L. 120-2 of the French Labor Code authorizes employer restrictions on employee rights as long as the restriction is proportionate.[330] This

323. ECHR, *supra* note 240, art. 8.

324. C. CIV., art. 9 (establishing that everyone has a right to privacy).

325. N.C.P.C., art. 9 (noting that each party is responsible for proving the necessary facts to establish their claims under the law).

326. C. TRAV., art L. 120-2 (prohibiting restrictions on personal rights and on individual and collective freedoms unless it is justified by the nature of the task to be accomplished and proportionate to the objectives achieved by the restriction).

327. Cass. soc., Dec. 11, 2001, 2001 Bull. Civ. V, No. 377; *see also* Waquet II, *supra* note 314, at 7.

328. Cass. soc., Dec. 11, 2001, 2001 Bull. Civ. V, No. 377.

329. *Id*.

330. C. TRAV., art. L. 120-2.

balancing test approach is also taken by article 7(f) of Directive 95/46, the case law of the ECHR, and common law in the United States.[331]

What is innovative about *Nikon France* is its application of the principle of proportionality. According to the European and American approaches, including French case law before *Nikon France*, an employer in the private sector may legally monitor the personal e-mail of employees sent during business hours as long as there is advance notice of the monitoring.[332] This means that the interests of an employer prevailed so long as advance notice was given. The court in *Nikon France*, on the other hand, considered complete access to personal messages to be disproportionate. Thus, the decision prohibits an employer from having unlimited access to personal e-mail, unless exceptional circumstances exist,[333] because personal e-mail is protected by the right of secrecy of correspondence, which forms a part of the right to privacy in the workplace during business hours.[334] In this sense, *Nikon France* puts the interests of employee above those of an employer.

In addition to its prohibition on unlimited e-mail access, *Nikon France* addressed one more facet of the principle of proportionality. In its decision, the court added that an employer cannot access personal messages even when they have prohibited the use of office computers for non-professional purposes.[335] In *Nikon France*, the Attorney General of the Court of Cassation discussed in his conclusion (a final statement given as a recommendation of judgment that often influences the court's decision) the impact of social change and the potential for dilution of the office/residence distinction.[336] The Attorney General concluded that a total prohibition on computer use for non-professional purposes would be unrealistic.[337] The French National Commission of Computers and Freedom issued a report in March 2001 reaching the same conclusion as

---

331. Directive 95/46, *supra* note 11, art. 7(f); Halford v. United Kingdom, 1997-III Eur. Ct. H.R. 1004 (1997); *see supra* notes 119–21 and accompanying text.

332. *See supra* Part III.

333. The Attorney General of the Court of Cassation suggests that the court will strictly interpret "exceptional circumstances," because they are "the conditions extremely demanding." Kehrig, *supra* note 317, at 8.

334. Cass. soc., Oct. 2, 2001, 2001 Bull Civ. V, No. 291, at 233–34.

335. *Id.*

336. Cass. soc., Oct. 2, 2001, 2001 Bull Civ. V, No. 291 (statement of the Attorney General), *at* http://www.courdecassation.fr/arrets/visu.cfm?num=1500 (last visited Feb. 2, 2005).

337. *Id.*; Kehrig, *supra* note 317, at 8. On the other hand, some commentators suggest that an employer could still introduce the total prohibition policy, in spite of the Attorney General's statement. *See*, *e.g.*, Ariane Mole, *Débat autour de l'Arrêt Nikon France: Entretien* [*Debate around the Judgment of Nikon France: Interview*], 1046 SEM. SOC. LAMY 12, 12 (2001).

the Attorney General.[338] Given that an employee has a right to privacy even during business hours, the Attorney General in this case correctly stated that a total prohibition is disproportionate. Accordingly, after *Nikon France*, during business hours, an employer must tolerate modest computer use for non-professional purposes, including personal e-mail, and the employer cannot access that personal e-mail.[339]

Under *Nikon France*, employers and employees must come to an accord in developing a monitoring policy that does not violate employee privacy.[340] For example, employers and employees might agree on a policy that stipulates employees may use only free Web-based e-mail for personal communications, and that office e-mail addresses are to be used only for professional communications. Employers could then monitor communications sent through office e-mail addresses, and monitor the time employees spend on Web-based e-mail websites for their own productivity and employee discipline purposes.

2. Corporate Scandals in the United States

During the last few years, the United States suffered a series of corporate scandals in which U.S. companies committed major acts of accounting fraud. Two of the largest scandals involved Enron and WorldCom.

Enron, a Houston company, was created in 1985 after Houston Natural Gas merged with InterNorth.[341] Initially, Enron was doing business only in pipeline gas and power.[342] However, Enron later expanded its projects beyond gas and power to take on business outside the United States.[343] Enron became a market-maker for energy-related products through a process of taking commissions from market participants.[344] This strategy left Enron with an enormous debt that it did not want to disclose, as investors would lose their confidence in Enron and its stock price would

338. COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS [NATIONAL COMMISSION OF COMPUTERS AND FREEDOM], 21ÈME RAPPORT D'ACTIVITÉ: 2000 [21ST REPORT OF ACTIVITY: 2000], 133 (2001).

339. This tolerance, inspired by the social changes, probably influenced the aforementioned application of the balancing test in *Nikon France*.

340. Cass. soc., Oct. 2, 2001, 2001 Bull Civ. V, No. 291, at 234.

341. *Enron: Timeline, 1985: Founding Years*, BBC NEWS, *at* http://news.bbc.co.uk/hi/english/static/in_depth/business/2002/enron/timeline/1.stm (last visited Nov. 17, 2004).

342. *Id.*

343. *Id.*

344. *Enron: Timeline, 1990s: Market Making*, BBC NEWS, *at* http://news.bbc.co.uk/hi/english/static/in_depth/business/2002/enron/timeline/4.stm (last visited Nov. 17, 2004).

fall. If the stock price fell, the executives, who were also big shareholders, would lose substantial sums of money.

In order to hide this red ink, Enron established a financial entity into which it transferred these debts.[345] This enabled Enron to announce an inflated profit, thereby easing the anxiety of its investors. At the same time, the Enron executives sold their own stocks at the inflated prices.[346] Eventually, in 2001, Enron was forced to announce that it had committed accounting fraud, its stock price fell, and its employees lost their jobs.

WorldCom essentially took the same path as Enron. WorldCom was a regional telecommunication company in the 1980s.[347] As it rapidly grew and became international,[348] it incurred a huge debt[349] that it hid in the same manner as Enron.[350] These scandals have generated public distrust of employers, corporate executives, and directors in the United States. This distrust of employers raises the following question: How can employers manage employees when the employers cannot manage themselves? In the context of e-mail monitoring, this question was translated into a suspicion that employers were abusing their authority in monitoring e-mails of employees. Such a suspicion gave the United States an opportunity to limit e-mail monitoring by employers; unfortunately, this opportunity was not one of which U.S. authorities took advantage.

3. Comparative Prediction of the Future of Data Protection of Employees in the Private-Sector

While *Nikon France* has no direct legal effect on EU member states other than France, it will likely lead to an indirect increase in the level of employee data protection due to the limits it suggests should be placed on e-mail monitoring. First, the Court of Cassation in *Nikon France* issued an interpretation of legal authority that binds (or mirrors) laws that are binding in other EU member states. In particular, the decision interpreted article 8 of the ECHR, article 9 of the French Civil Code, and article L. 120-2 of the French Labor Code, all of which bind or mirror binding

345. Tom Fowler, *The Pride and the Fall of Enron*, HOUS. CHRON., Oct. 20, 2002, at A1, *available at* 2002 WL 23231814.

346. *Enron's Collapse: How Enron Fell: Insider Trading*, N.Y. TIMES, *at* http://www.nytimes.com/packages/html/business/20020115_enron_FALL/biz_enron_FALL_02.html (last visited Nov. 17, 2004).

347. *U.S. Telecoms Giant Admits Huge Fraud*, BBC NEWS, June 26, 2002, *available at* http://news.bbc.co.uk/1/hi/business/2066731.stm (last visited Nov. 17, 2004).

348. *Id.*

349. *Id.*

350. *Id.*

authority in other EU states.[351] For example, article 8 of the ECHR, which guarantees a right to privacy, is operative in every member state of the European Union.[352] Article 9 of the French Civil Code protects the privacy of individuals from invasion by other private parties.[353] Directive 95/46 similarly protects a private individual's privacy from invasion by another through its application to the private-sector.[354] Article 6(c) of Directive 95/46 adopts the principle of proportionality in a fashion similar to article L. 120-2 of the French Labor Code.[355] Furthermore, article 7(f) of Directive 95/46 parallels article L. 120-2 in its attempt to balance the interests of an employer and an employee in the workplace.[356] Thus, the similarity of these substantive provisions indicates that interpretation of the legal principles in Directive 95/46 may parallel the interpretation by the French court.

Second, key to this prediction is the recognition of a right to privacy in the workplace. In *Nikon France*, the Court of Cassation recognized an employee's right to privacy in the workplace during business hours. This right to privacy in the workplace, along with other social changes, has driven an innovative application of the balancing of employer and employee interests. Like France, Western Europe, in general, has tended to recognize the right to privacy in the workplace, and the social changes mentioned by the Attorney General of the Court of Cassation are to be found across Western Europe.[357]

Thus, the courts in other member states of the European Union would likely reach the same analysis as that employed in *Nikon France*. These courts would thus conclude that an employer may monitor personal e-mail only under exceptional circumstances, and that a violation of this rule

351. Cass. soc., Oct. 2, 2001, Bull Civ. V, No. 291, at 233–34.
352. ECHR, *supra* note 240, art. 8.
353. C. CIV., art. 9.
354. Directive 95/46, *supra* note 11, art. 3.
355. *Id.* art. 6(c); C. TRAV., art. L. 120-2.
356. Directive 95/46, *supra* note 11, art. 7(f).
357. The Article 29 Working Party of the European Union, aware of the right to privacy in the workplace and the social changes mentioned in *Nikon France*, interprets the principle of proportionality to mean that employers should always process personal data in the least intrusive manner possible, while considering the risks at stake, the amount of data involved, the purpose of the processing, etc. ARTICLE 29 WORKING PARTY, *supra* note 87, at 21. This interpretation requires a strict application of the proportionality to a particular situation. Thus, negotiations into the representatives of workers on the method of surveillance and the usage of "new technologies" is inevitable under the European Data Protection Directive. Olivier Rijkaert, *Cyber Surveillance des Salaríes: l'Étau Se Resserse Suite á Un Arrêt de Cassation Francais* [*Cyber Surveillances of Employees: Tightens After a Judgment of French Supreme Court*], Oct. 15, 2001, *at* http://www.droit-technologie.org/1_2.asp?actu-id=471 (last visited Nov. 17, 2004).

justifies sanctioning the employer. Additionally, given the greater role that the government in Western Europe tends to play, it is possible that Western European countries will limit e-mail monitoring legislatively.

Conversely, the United States is unlikely to increase the protection of employee privacy in the private-sector despite the opportunity to do so that was presented by U.S. corporate scandals. Because the United States does not accord the right to privacy as high a status as Western European countries, courts in the United States are unlikely to apply the balancing test in the same way as the Court of Cassation did in *Nikon France*. In other words, the interests of an employer will continue to prevail over those of an employee. It is also unlikely that the United States will legislate greater data protection for private-sector employees. The government is reluctant to intervene in private-party relationships and any attempt to intervene would encounter the strong resistance of lobbyists, financed by employers who oppose the increased costs associated with a greater level of data protection.[358] In addition, before any legislation to increase protection of employer privacy was enacted, public outrage against employers—the only force likely to overcome the powerful lobbyists working against such legislation—was quickly replaced by public outrage against the terrorists who perpetrated the tragedy of September 11, 2001.

In summary, in Western Europe, the level of data protection of private-sector employees is likely to increase in the future. In contrast, the level of protection will likely stay the same in the United States.

V. CONCLUSION

Western Europe and the United States have each built data protection schemes around a legislative source: Directive 95/46 and the ECPA, respectively. Case law at the European level allows an employer, in some circumstances, to monitor employee e-mail. The exceptions to the ECPA and the common law show that the United States presently reaches a result similar to that in Western Europe. However, following *Nikon France*, Western Europe is likely to protect data privacy and increasingly limit e-mail monitoring because of the greater value that Western Europe places on the right to privacy and the greater role Western European governments play as a guarantor of citizens' rights. On the other hand, in the United States, society is skeptical of governmental intervention and the status of

358. Charlesworth, *supra* note 13, at 83.

the right to privacy is lower than in Western Europe. Corporate scandals spread fear of employers abusing their authority and may have provided a significant opportunity to increase employee privacy. This opportunity, however, appears to have passed, and the level of data protection in the United States will likely remain the same in the future.