



## Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada

GAIL LASPROGATA, NANCY J. KING, SUKANYA PILLAY<sup>□</sup>

CITE AS: 2004 STAN. TECH. L. REV. 4

[http://stlr.stanford.edu/STLR/Articles/04\\_STLR\\_4](http://stlr.stanford.edu/STLR/Articles/04_STLR_4)

¶1 This article is dedicated with warm appreciation to Professor Richard Turkington, an accomplished and innovative privacy law scholar and an inspirational teacher to all his law students who loved him dearly.

### I. INTRODUCTION

¶2 The Information Age has radically altered the traditional legal and organizational framework of work by blurring the once clear boundaries between an employee's personal and professional lives. Employees experience increased autonomy and flexibility both at work and at home with the increase in telecommuting and "mobile" working.<sup>1</sup> These advances are aptly facilitated by appropriate information systems and tools supplied by employers. However, these same systems and tools facilitate the intrusion of professional life into the personal sphere, and sometimes the intrusion of the employer into the private lives of its employees.

---

<sup>□</sup> Gail Lasprogata is an assistant professor at Seattle University. Nancy King is an assistant professor at Oregon State University. Sukanya Pillay is an assistant professor at the University of Windsor.

<sup>1</sup> THE INTERNET RIGHTS FORUM, WORKING RELATIONSHIPS AND INTERNET (Final Report, Sept. 17, 2002), at [http://www.foruminternet.org/telechargement/documents/rapp-rti-20020917\\_en.htm](http://www.foruminternet.org/telechargement/documents/rapp-rti-20020917_en.htm) [hereinafter IRF Final Report]. The Internet Rights Forum is a private body supported by the French government that invites the input of all the actors on the Internet (private companies, non-profit organizations, public authorities and users) to discuss and suggest uses and rules for online activity. See also Joan T. A. Gabel and Nancy R. Mansfield, *The Information Revolution and Its Impact on the Employment Relationship: An Analysis of The Cyberspace Workplace*, 40 AM. BUS. L.J. 301 (2003) (giving an extensive overview of how the Information Revolution has altered the employment relationship in the United States). For statistics on the use of information technologies in the European Union, see European Industrial Relations Observatory Online, *New Technology and Respect for Privacy at the Workplace*, at <http://www.eiro.eurofound.eu.int/2003/07/study/tn0307101s.html> (last visited Jan. 30, 2003) [hereinafter, Eironline Study]. Technological advances are not necessarily in the best interest of the employee's psychological well-being. See, e.g., NOELLE CHESLEY, LIVING IN A NANOSECOND WORLD: TECHNOLOGY USE, TIME AND PSYCHOLOGICAL WELL-BEING IN DUAL EARNER COUPLES (Bronfenbrenner Life Course Center Working Paper 01-05) (Mar. 2001) (Cornell Employment and Family Careers Institute) (discussing linkages between use of technology and dissatisfaction with personal and family life). Cf. Stephan DESROCHERS & LEISA D. SARGENT, BOUNDARY/BORDER THEORY AND WORK-FAMILY INTEGRATION (2002), at [http://www.bc.edu/bc\\_org/avp/wfnetwork/rft/wfpedia/wfpBBTent.html](http://www.bc.edu/bc_org/avp/wfnetwork/rft/wfpedia/wfpBBTent.html); Douglas T. Hall & Judith Richter, *Balancing Work and Home Life: What Can Organizations Do to Help?*, 2 ACAD. MGMT. EXECUTIVE No. 3, at 213 (Aug. 1988) (proposing that work and home should be separated, not integrated).

¶3

Employers increasingly are using electronic monitoring technologies to observe what employees do on the job and to review their electronic communications.<sup>2</sup> Employee advocates argue that electronic monitoring practices have significantly eroded employee privacy rights.<sup>3</sup> However, employers assert there are many good business reasons to electronically monitor employees in the workplace, including:

To monitor employee productivity in the workplace.<sup>4</sup>

To maximize productive use of the employer's computer system when employees use computers on the job.<sup>5</sup>

To monitor employee compliance with employer workplace policies related to use of its computer systems, email systems, and Internet access.<sup>6</sup>

To investigate complaints of employee misconduct, including harassment and discrimination complaints.<sup>7</sup>

To prevent or detect industrial espionage, such as theft of trade secrets and other proprietary information, copyright infringement, patent infringement, or trademark infringement by employees and third parties.<sup>8</sup>

To prevent or respond to unauthorized access to the employer's computer systems, including access by computer hackers.<sup>9</sup>

---

<sup>2</sup> Camille L. Hébert, *Methods and Extent of Employer Use of Electronic Monitoring and Surveillance*, EMPLOYEE PRIVACY LAW § 8A-1 (2002). Hébert summarizes recent surveys of the prevalence of employer electronic monitoring and surveillance including: 1) the 2001 Workplace Monitoring and Surveillance Survey by the American Management Association Survey that reported 46.5% of respondents reviewed employee electronic mail messages, 7.8% reviewed employee voice mail messages, 36.1% reviewed employee computer files, and 62.8% monitored employee Internet connections; and 2) the Society for Human Resources Management Survey that reported "80% of the respondents have or use electronic mail systems and 36% of those with such systems review their employees' email." *Id.* See also American Management Association, *2003 E-Mail Rules, Policies and Practices Survey* (2003), available at <http://www.amanet.org> (last visited Dec. 10, 2003). A 2002 survey in the United Kingdom concluded that employers spent more time disciplining staff over Internet and email abuse than any other workplace issue. The three most common problems were excessive personal use of the Internet and email, sending pornographic messages, and looking at pornographic websites. See Eironline Study, *supra* note 1.

<sup>3</sup> Additional arguments against employee electronic monitoring focus on the effects on employee morale, the trust relationship with the employer, and the ultimate effect on work product. See, e.g., Sonny S. Ariss, *Computer Monitoring: Benefits and Pitfalls Facing Management*, 39 INFO. & MGMT. 553, 556-557 (2002).

<sup>4</sup> Paul E. Hash & Christina M. Ibrahim, *E-Mail, Electronic Monitoring, and Employee Privacy*, 37 S. Tex. L. Rev. 893, 897 (1996).

<sup>5</sup> Elise M. Bloom et al., *Competing Interests in the Post 9-11 Workplace: The New Line Between Privacy and Safety*, 1317 PRACTICING L. INST./CORP. 303 (2002). According to Bloom et al.:

Employers have always monitored their employees, whether for reasons of efficiency, security, or legal obligation. Title VII of the Civil Rights Act of 1964, as amended, as well as a myriad of other state and federal laws, impose on employers an obligation to monitor the workplace to take measures to ensure that the workplace is harassment-free. An employer's communication systems are generally considered part of the workplace since they are used by employees during working time on working premises. However, with the influx of better technology, the extent and ability to monitor have increased dramatically. As businesses rely more and more on electronic mail . . . and electronic communications such as voice mail and mobile phones, employers have many new outlets to monitor their employees. A report last year by the Privacy Foundation stated that fourteen million employees, just over one-third of the online workforce in this country, had their email or internet use continuously monitored at work.

*Id.* at 309. See also Brian P. Kane, *1984 In 2001: Monitoring Employee E-mail Usage*, 44 ADVOC. (IDAHO) 20, 21 (September, 2001) (listing numerous reasons why employers should monitor employees' Internet and email communications).

<sup>6</sup> New Technologies, Inc., *Employee Wrongful Dismissal Lawsuits*, at <http://dataforensics.com/law11.html> (last visited Aug. 11, 2003) (discussing the prevalence of employee dismissals result from inappropriate behavior on a company owned personal computer or computer network).

<sup>7</sup> Advances in electronic technology have expanded the avenues of employee communications in the workplace and the potential forms of employee misconduct, giving rise to new investigatory obligations on the part of employers. Racial or sexual harassment through email communications, and the ability to download or view pornography in the workplace on employer-provided computers, are relatively new ways that employees may violate employment policies and discrimination laws. See *Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 98-99 (E.D. Pa. 1996) (discussing a case where employee used email to communicate unprofessional comments criticizing management of the company); LEE B. BURGUNDER, LEGAL ASPECTS OF MANAGING TECHNOLOGY 493 n.42 (2nd ed. 2001) (citing a recent study showing employees at three major U.S. companies visited Penthouse's web site 12,825 times in a single month in 1996).

<sup>8</sup> Mike Consol, *Industrial Espionage, The Secret Agents of Fortune*, BUS. J. (1998), at <http://www.secure-data.com/art9.html> (last visited Aug. 11, 2003).

<sup>9</sup> Institute for Security Technology Studies at Dartmouth College, *Law Enforcement Tools and Technologies for Investigating Cyber Attacks, A National Needs Assessment* (2002), at [http://www.ists.dartmouth.edu/TAG/needs/ISTS\\_NA.pdf](http://www.ists.dartmouth.edu/TAG/needs/ISTS_NA.pdf) (last visited Aug. 11,

To protect computer networks from becoming overloaded by large downloadable files.<sup>10</sup>

To prevent or detect unauthorized utilization of the employer's computer systems for criminal activities and terrorism.<sup>11</sup>

To help prepare the employer's defense to lawsuits or administrative complaints such as those brought by employees related to discrimination, harassment, discipline, or termination of employment.<sup>12</sup>

To respond to discovery requests in litigation related to electronic evidence.<sup>13</sup>

¶4

U.S. employers can be confident that electronic employee monitoring will in most cases receive the sanction of state and federal law. However, multinational employers face a potentially daunting task in complying with more sophisticated, and possibly more stringent privacy protection afforded to their employees abroad. Current law reveals global variations in the substance and practical application of data privacy requirements.<sup>14</sup> Regional, federal, and local authorities that share in the formulation and application of data privacy law exacerbate the complexity of the jurisdictional issues for multinational employers.<sup>15</sup> Added to the maze of intricacies is the application of relevant labor and employment law requiring, in some cases, the consent of multiple employee representative groups to the implementation of any new technology that affects working conditions.

¶5

This paper compares the regulation of electronic employee monitoring in the European Union (EU)<sup>16</sup>, the United States, and Canada and attempts to reconcile conflicting legal standards regarding workplace privacy as they are evolving in the wake of technological advances and managerial needs. Section II paints the landscape of "the right to privacy" and compares cultural and political variations in interpreting that right between the EU, the United States, and Canada. Also included is a synopsis of how the right to privacy and the employment relationship have been altered by recent changes in technology that facilitate the collection, processing, and dissemination of personal information and communications. Sections III, IV, and V explain the current regulation of electronic monitoring of employees in the EU, the United States, and Canada respectively. Section VI then draws out the major privacy principles that emerge from a review of the relevant regulatory law in these jurisdictions. This section also offers an examination of the practical application of these fundamental privacy principles across the EU, the United States, and Canada, and reveals for

---

2003).

<sup>10</sup> IRF Final Report, *supra* note 1, at 17.

<sup>11</sup> A. HUGH SCOTT, COMPUTER AND INTELLECTUAL PROPERTY CRIME: FEDERAL AND STATE LAW 141 (2001); KENNETH S. ROSENBLATT, HIGH-TECHNOLOGY CRIME 1-3 (1995); Michael R. Anderson, *Identifying Internet Activity, Computer Forensics Goes to Cyber Space*, at <http://www.forensics-intl.com/artipfl.html> and *Net Threat Analyzer*, at <http://www.forensics-intl.com/nta.html> (last visited Aug. 11, 2003) (describing Net Threat Analyzer software and its use to detect terrorism threats).

<sup>12</sup> Monique C.M. Leahy, *Recovery and Reconstruction of Electronic Mail as Evidence*, 4 AM. JUR. 3D *Proof of Facts* § 1 (2002); William Decoste, *Sender Beware: The Discoverability and Admissibility of E-Mail*, 2 VAND. J. ENT. L. & PRAC. 79, 81 (2000); . See also *Strauss v. Microsoft Corp.*, 1995 U.S. Dist. Lexis 7433, at \*4-\*5 (S.D.N.Y. 1995). In *Strauss*, Microsoft was sued for sex discrimination and wrongful discharge by an employee who had received email messages from her supervisor. *Id.* at \*6-\*7. The emails referred to a female co-worker as "Spandex Queen" and himself as "president of the Amateur Gynecology Club." *Id.* at 10. The court held these email messages were admissible evidence and a jury could conclude that the company's stated reason for failing to promote the employee was not the true reason for its actions, but rather her sex was the reason. *Id.* at 14.

<sup>13</sup> Albert Barsocchini, *Electronic Discovery Primer*, 20-8 MATRIMONIAL STRATEGIST 7 (2002). See also Leahy, *supra* note 12, at 1.

<sup>14</sup> See Vincent Serpico, Denise Landers & Damon Terrill, *A Guide to Managing Multi-Jurisdictional Data Privacy Law Matters for Financial Services Companies*, PLI Order N. G0-01A2 715 (June, 2003).

<sup>15</sup> See *id.*

<sup>16</sup> The European Union (EU) was set up after the 2nd World War. The process of European integration was launched on May 9, 1950 when France officially proposed to create "the first concrete foundation of a European federation." *Declaration of 9 May, 1950*, at [http://europa.eu.int/abc/symbols/9-may/decl\\_en.htm](http://europa.eu.int/abc/symbols/9-may/decl_en.htm) (last visited Dec. 11, 2004). Six countries (Belgium, Germany, France, Italy, Luxembourg and the Netherlands) joined from the very beginning. Today, after four waves of accessions (1973: Denmark, Ireland, and the United Kingdom; 1981: Greece; 1986: Spain and Portugal; 1995: Austria, Finland, and Sweden) the EU has 15 member states and is preparing for the accession in 2004 of 10 new countries. See The European Union's Official Website, *The European Union at a Glance*, at [http://www.europa.eu.int/abc/index\\_en.htm](http://www.europa.eu.int/abc/index_en.htm) (last visited Jan. 26, 2004) [hereinafter, *Europa*]. See also Ursula R. Kubal, U.S. *Multinational Corporations Abroad: A Comparative Perspective on Sex Discrimination Law in The United States and the European Union*, 25 N.C. J. INT'L L. & COM. REG. 207 (1999) (providing an overview of the EU political and legal framework, including the founding treaties, institutions and sources of law); Roger J. Goebel, *The European Union Grows: The Constitutional Impact of the Accession of Austria, Finland and Sweden*, 18 FORDHAM INT'L L.J. 1092 (1995).

employers the parameters of employee privacy protection where electronic monitoring is a desired management practice. Section VII concludes with a recommendation that employers honor the fundamental privacy principles derived from the comparative analysis. Although not yet universally required, the privacy principles collectively create an equitable paradigm that rightfully protects employee dignity while recognizing the legitimate management needs of employers.

## II. THE LANDSCAPE

### A. *The Right to Privacy*

¶6 Privacy is "the right to be let alone."<sup>17</sup> It is universally recognized as an individual, personal right of philosophical and moral origins.<sup>18</sup> What is included in that right is, however, often debatable as there are conflicting interpretations of what types of privacy warrant legal recognition and protection.<sup>19</sup> Historically protected areas include informational privacy (the right to be let alone with respect to one's personal information)<sup>20</sup>, physical privacy (the right to be let alone with respect to one's person and surrounding environment)<sup>21</sup>, and decisional privacy (the right to be let alone with respect to one's personal decisions).<sup>22</sup>

¶7 American notions of privacy are reflected in the concept of "rugged individualism."<sup>23</sup> Individual autonomy and liberty are revered, as is apparent in the jurisprudence of decisional privacy.<sup>24</sup> However, the right to privacy is treated as akin to personal property.<sup>25</sup> As such, it may be bargained

<sup>17</sup> Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). Cf. Matthew Finkin, *Privacy and Employment Law*, (John D.R. Craig), 21 COMP. LAB. L. & POL'Y J. 813, 815 (2000) (book review). The concept of privacy is inextricably entwined with individual autonomy. Some believe that there is in fact "no general privacy principle, but rather a set of privacy principles, a cluster of related concerns or interests that are context-specific." *Id.*

<sup>18</sup> The Universal Declaration of Human Rights states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." Dec. 10, 1948, art. 12, U.N. G.A. Res. 217, (III 1948). This same right is incorporated into the International Covenant on Civil and Political Rights in Article 17, 999 U.N.T.S. 171, Dec. 16, 1966. The American Convention on Human Rights states: "Everyone has the right to have his honor respected and his dignity recognized." Article 11, par. 1 9 I.L.M. 673 (1970). The United States has not ratified this convention.

<sup>19</sup> See Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085 (2002). Lin describes definitions of privacy that have been put forth by other scholars:

Jerry Kang describes three "clusters" – privacy concerns with regard to (1) physical space ("spatial privacy"), (2) choice, and (3) the flow of personal information. . . . Anita Allen-Castellitto divides privacy into "at least four basic types": (1) informational privacy, (2) physical privacy, (3) decisional privacy, and (4) proprietary privacy. . . . Meanwhile, the fathers of privacy law, Samuel Warren and Justice Louis Brandeis, described a "general right to privacy for thoughts, emotions, and sensations [that] should receive the same protection, whether expressed in writing, or in conduct, in conversation, in attitudes, or in facial expression."

*Id.* at 1093-94 (citations omitted).

<sup>20</sup> *Whalen v. Roe*, 429 U.S. 589, 598-600 (1977) (separating the constitutional right to privacy into at least two interests including the individual interest in avoiding disclosure of personal matters and the interest in independence in making certain types of decisions). See also Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501-03 *et seq.* (2003), Gramm-Leach-Bliley (GLB) Act, 15 U.S.C. §§ 6801-27 (2003) (requiring financial institutions to notify consumers of their privacy policies but authorizing financial institutions to share consumers' nonpublic personal information with related affiliates); Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (2003) (codified as amended in scattered sections of 29 U.S.C. and 42 U.S.C.); The Privacy Act of 2003, S. 745, 108th Cong. (2003) (proposed legislation that would set a national standard for protection of personal information, including Social Security numbers, driver's license numbers, and health and financial data).

<sup>21</sup> See U.S. CONST. amends. IV & XIV; *Kyllo v. United States*, 533 U.S. 27, 31 (2001) (applying the Fourth Amendment to electronic surveillance of a home using thermal imaging technology); *Silverman v. United States*, 365 U.S. 505, 511 (1961): "'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'" Cf. *R. v. Dymnt*, [1988] 2 S.C.R. 417 (Can) (blood sample improperly obtained by police held to be an invasion of personal privacy).

<sup>22</sup> See *Whalen*, 429 U.S. at 589, 598-600; *Griswold v. Connecticut*, 381 U.S. 479, 484-485 (1965) (finding a constitutionally related right to privacy arising from the "penumbra" of the First, Fourth, Fifth, Ninth and Fourteenth Amendments).

<sup>23</sup> Jay P. Kesan, *Cyber-Working or Cyber-Shrinking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 306 (2002).

<sup>24</sup> *Lawrence v. Texas*, 123 S.Ct. 2472 (2003) (right to engage in consensual act of sodomy in private home protected); *Whalen*, 429 U.S. at 589; *Roe v. Wade*, 42 U.S. 113 (1973) (right to abortion protected); *Loving v. Virginia*, 388 U.S. 1, 12 (1967) (right to marry protected); Kesan, *supra* note 23, at 306.

<sup>25</sup> Kesan, *supra* note 23, at 306; William A. Wines and Michael P. Fronmueller, *American Workers Increase Efforts To Establish A*

and exchanged for other rights and privileges, including those obtained in an employment relationship.<sup>26</sup> In other words, since privacy belongs to the individual, it may be traded away by the individual in exchange for something of commensurate value, such as a job.

¶8 American law in this area stands apart from most of the world, which starts instead from the position that the right to privacy is a central tenet of human dignity.<sup>27</sup> Human dignity means "being accorded the respect and status appropriate to a human being, being treated in a way that allows or enables one to live a becoming existence."<sup>28</sup> Unlike proprietary privacy rights, human dignity is not generated by the individual, but is instead created by one's community and bestowed upon the individual.<sup>29</sup> It cannot therefore be bartered away or exchanged under traditional notions of at-will employment and contract law as seen in U.S. law.<sup>30</sup>

¶9 This philosophy is largely adhered to in Europe, where the right to privacy is elevated to the status of a fundamental right.<sup>31</sup> Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms states: "Everyone has the right to respect for his private and family life, his home and his correspondence."<sup>32</sup> The Treaty of the European Union recognizes this Convention and requires Member States to respect the fundamental rights guaranteed therein.<sup>33</sup> The more recent Charter of Fundamental Rights of the European Union affirms that "[e]veryone has the right to respect for his or her private and family life, home and communications."<sup>34</sup>

---

*Legal Right to Privacy as Civility Declines in U.S. Society: Some Observations on the Effort and Its Social Context*, 78 NEB. L. REV. 606 (1999). Canada recognizes a dimension of territorial privacy that derives from British common law interpretations or property rights wherein an individual in his home is protected against trespass or unlawful state intrusion.

<sup>26</sup> See Kesan, *supra* note 23, at 306-07.

<sup>27</sup> See *id.* at 307. See also Wines & Fronmueller, *supra* note 24, at 623-28.

<sup>28</sup> Wines & Fronmueller, *supra* note 24, at 623.

<sup>29</sup> See Kesan, *supra* note 23, at 307.

<sup>30</sup> Employment at-will is a doctrine that allows employers to discharge an employee for almost any reason or for no reason, as long as the discharge is not contrary to a statute or a contract. □ Edwin Robert Cottone, Comment, *Employee Protection from Unjust Discharge: A Proposal for Judicial Reversal of the Terminable-At-Will Doctrine*, 42 SANTA CLARA L. REV. 1259, 1259 (2002). □ Theoretically, the at-will doctrine is based on viewing the relationship between employer and employee as a mutual relationship where either the employer or employee is free to terminate the relationship at any time. □ *Id.* □ Some notable exceptions to employment at-will mitigate the harshness of the at-will doctrine, such as federal or state discrimination laws. □ *Id.* at 1268-69. □ For example, it is unlawful under federal discrimination laws for an employer to treat employees differently with respect to terms and conditions of employment based on their sex, race, color, national origin, religion, age, or disability. □ *Id.* □ Generally speaking, many private sector employees in the U.S. are at-will employees who give up any rights to privacy in the workplace by agreeing to work for the employer. □ Lawrence E. Rothstein, *Privacy or Dignity: Electronic Monitoring in the Workplace*, 19 N.Y.L. SCH. J. INT'L & COMP. L. 378, 382-83 (2000). □ See also Stan Malos et al., *A Contingency Approach to the Employment Relationship: Form, Function, and Effectiveness Implications*, 15 EMP. RESP. RTS. J. 149, 149 (2003) (comparing the U.S., Canadian, and New Zealand approaches to employment relationships). □ While at-will employment relationships are common in the United States, they are not the basis of employment relationships in much of the rest of the world. □ *Id.* at 156. Cf. John T. Addison & Clive R. Belfield, *What Do We Know About the New European Works Councils? Some Preliminary Evidence from Britain*, 49 SCOT. J. POL. ECON. 418 (2002) (discussing the requirement of multinational employers to consult with worker representatives under the 1994 Works Council Directive); Tony Royle, *Worker Representation Under Threat? The McDonald's Corporation and the Effectiveness of Statutory Works Councils in Seven European Union Countries*, 22 COMP. LAB. L. & POL'Y J. 395 (2001) (describing unionization rules in the EU); Madeleine M. Plasencia, *Employment-At-Will: The French Experience as a Basis for Reform*, 9 COMP. LAB. L.J. 294 (1988) (discussing French dismissal law). □ In Canada the employment relationship is viewed as contractual and generally requires reasonable notice before termination of employees or compensation in lieu thereof. See generally GEOFFREY ENGLAND, *ESSENTIALS OF CANADIAN LAW: INDIVIDUAL EMPLOYMENT LAW* (2000). Canadian employees must also give the employer reasonable notice of their intent to leave employment. □ However, upon termination, even at-will employees in the U.S. may have remedies that far exceed those available to employees in countries that do not recognize at-will employment. □ See Malos et al., *supra*, at 151. □ Many of these monetary remedies relate to *how* employers handle terminations, not whether an employer can terminate an employee without advance notice. □ *Id.* □ Even at-will employees may recover monetary damages for the torts of defamation, invasion of privacy, intentional infliction of emotional distress, and constructive discharge, depending on how the employee was terminated. □ *Id.*

<sup>31</sup> This approach to privacy has deep roots in the civil law tradition. Many European countries include the right to personal data privacy in their constitutions. See Barbara Crutchfield George et al., *U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive*, 38 AM. BUS. L.J. 735, 743 (2001).

<sup>32</sup> Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, art. 8, para. 1, 213 U.N.T.S. 221.

<sup>33</sup> TREATY ESTABLISHING THE EUROPEAN COMMUNITY, Feb. 7 1992, O.J. (C 224) 1 (1992).

<sup>34</sup> CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION, art. 7, Dec. 7, 2000, O.J. (C 364) 1 (2000). Use of the word "communications" is intended to take into account advances in technology that are not obviously reflected in the word "correspondence." Eironline Study, *supra* note 1.

- ¶10 Canada likewise defines the right to privacy as a fundamental right.<sup>35</sup> Although privacy is not a right specifically guaranteed by the Canadian Charter of Rights and Freedoms, the notion of a right to privacy emerges from democratic ideals regarding the individual, the state, and the fundamental freedoms requisite to democracy. In Canada, the highest court has held that "privacy is at the heart of liberty in a modern [democratic] state."<sup>36</sup>
- ¶11 With the evolution of new computer technologies, the focus in recent years has been on the right to informational privacy, which includes the protection of personal information from the unwarranted intrusion by others.<sup>37</sup> In Canada, the right to informational privacy has been described as "the right of the individual to determine for himself when, how, and to what extent he will release personal information about himself."<sup>38</sup> Europeans define this right in terms of "personal data."<sup>39</sup>
- ¶12 The modern history of data privacy protection in Europe began in the 1970s with the early growth stages of the computer industry, which introduced a "technological dimension" to the right of privacy.<sup>40</sup> The 1980's saw the introduction of two leading international documents: the Organization for Economic Cooperation and Development's (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*<sup>41</sup> and the Council of Europe's 1981 *Convention for the Protections of Individuals with Regard to Automatic Processing of Personal Data*.<sup>42</sup> These instruments recognized the development of automatic data processing and the consequent need to consider privacy protection specifically in relation to the collection, storage and use of personal data through automatic means, including sensitive data regarding political and religious opinions, racial origin, health, and sexual orientation.<sup>43</sup>
- ¶13 The OECD Guidelines and the 1981 Council of Europe Convention each incorporate rules that require personal data protection from collection through dissemination, and guarantee the right of individuals to access information collected about them and make changes where necessary to correct inaccuracies. They call on nations to adopt privacy protection legislation, discourage restrictions on the flow of data among member nations to the OECD or the Council of Europe as the case may be, and support restrictions on the transfer of data to countries that do not provide adequate privacy protection.<sup>44</sup> In essence, these two international instruments foreshadowed what was to come in 1995 when the European Union adopted Directive 95/46/EC of the European Parliament and of

<sup>35</sup> See *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403, para. 65 (Can.). Canada is also a party to the International Covenant on Civil and Political Rights, *supra* note 17.

<sup>36</sup> Referring to La Forest's quote in *R. v. Dymnt* [1988] 2 S.C.R. 417, para. 28 (Can.), the Canadian Privacy Commissioner stated, "To me that's almost self-evident: How can we be truly free if our every move can be watched, our every activity known, our every preference monitored?" George Radwanski, Speech at the Spanish Data Protection Authority and Latin-American Centre of Data Protection Conference (May 20, 2002), available at [http://www.privcom.gc.ca/speech/02\\_05\\_a\\_020520\\_e.asp](http://www.privcom.gc.ca/speech/02_05_a_020520_e.asp).

<sup>37</sup> "Informational privacy is a right to understand the real and perceived consequences of the disclosure of personal information." Lin, *supra* note 18, at 1099.

<sup>38</sup> *R. v. Duarte*, [1990] 1 S.C.R. 30, para. 27 (Can.).

<sup>39</sup> See, e.g., Data Privacy Directive, Council Directive 95/46/EC, 1995 O.J. (L 281) [hereinafter EU Privacy Directive].

<sup>40</sup> George et al., *supra* note 30, at 744.

<sup>41</sup> The Guidelines are a set of non-binding rules for handling electronic data approved by members of the OECD, including the U.S. See *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD Doc. 58 (Sept. 23, 1980), available at <http://www.oecd.org> [hereinafter OECD Guidelines].

<sup>42</sup> See 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/cadreprincipal.htm> [hereinafter Council of Europe Convention]. In 1989 the Council of Europe Committee of Ministers adopted a Recommendation (R(89)2) on the protection of personal data used for employment purposes with the intent to adapt the Convention to the employment context. See Eironline Study, *supra* note 1, at 6. The Council of Europe is an international organization in Strasbourg, which comprises forty-four democratic countries in Europe. It was established by the Treaty of London on May 5, 1949. Membership is open to any European country that accepts the principle of the rule of law and guarantees human rights and fundamental freedoms to everyone in its jurisdiction. The Council considers all major issues facing European society other than defense. Its work programs include the following fields of activity: human rights, media, legal co-operation, social cohesion, health, education, culture, heritage, sport, youth, local democracy and transfrontier co-operation, the environment, and regional planning. *Id.*

<sup>43</sup> See, e.g., Council of Europe Convention, *supra* note 41, art. 6.

<sup>44</sup> George et al., *supra* note 30, at 744-45.

the Council on October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "EU Privacy Directive").<sup>45</sup>

¶14

As a result of the EU Privacy Directive, today there are national data protection laws in the member states that are administered by strong legal regimes charged with protecting citizens' personal data privacy.<sup>46</sup> The legislation is comprehensive, covering the full range of uses of personally identifiable information by both the public and private sectors.<sup>47</sup> The EU and its Member States have thus taken a very proactive approach to protecting personal privacy in light of the evolution of new computer technologies and the apparent need to protect privacy rights even across international borders.<sup>48</sup> Canada is following suit with its newly enacted federal Personal Information Protection and Electronic Documents Act (PIPEDA), which became widely effective on January 1, 2004.<sup>49</sup> PIPEDA was in fact inspired by the EU Privacy Directive and quite obviously uses the Directive as its paradigm.<sup>50</sup> In sharp contrast, the United States has taken a clearly reactive stance to the technology revolution.<sup>51</sup> The U.S. view is that there is enough of a "legal arsenal" in the form of existing legislation and judicial decisions to address privacy issues raised by new digital technologies without requiring new comprehensive legislative texts.<sup>52</sup>

¶15

With the advent of the Internet and prevalence of computerized databases, it has become more important to have a definition of privacy that includes informational privacy.<sup>53</sup> A right to informational privacy protects persons from privacy invasions that occur as a result of the use and disclosure of personal information gathered and stored in computerized databases, often gleaned from the Internet.<sup>54</sup> As this paper explores, the EU under the EU Privacy Directive defines

<sup>45</sup> The EU Privacy Directive became effective in 1998. EU Privacy Directive, *supra* note 38. Directives enact EU policy objectives. They require member states to enact or change relevant national law to achieve those objectives while allowing enough flexibility to retain national legal traditions. For these reasons, directives are the most prevalent form of EU law. See Kubal, *supra* note 16, at 214-15.

<sup>46</sup> See George et al., *supra* note 30, at 743.

<sup>47</sup> See Steven R. Salbu, *The European Union Data Privacy Directive and International Relations*, 35 VAND. J. TRANSNAT'L L. 655, 667 (2002). Most of the Member States of the EU have a civil law legal system where the role of case law is less relevant and the need for more precise legislation is mandated. See NICOLA LUGARESÌ, PRINCIPLES AND REGULATIONS ABOUT ONLINE PRIVACY: "IMPLEMENTATION DIVIDE" AND MISUNDERSTANDINGS IN THE EUROPEAN UNION 4 (TPRC Working Paper No. 42, 2002), available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=333440](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=333440) (last visited Jan. 31, 2004).

<sup>48</sup> See Salbu, *supra* note 47, at 666-67.

<sup>49</sup> Personal Information Protection and Electronic Documents Act, S.C., ch. 5 (2000) (Can.) [hereinafter, PIPEDA].

<sup>50</sup> See *infra* notes 276-95 and accompanying text.

<sup>51</sup> See Amr Zaki Abdel Motaal, *Privacy and the Information Systems (The Paradox and the Balance)*, Address Before the Public Voice in Emerging Market Economies Conference, OECD (Jan. 15, 2001), available at [http://www.thepublicvoice.org/events/dubai01/presentations/html/a\\_motaal/motaalpaper.html](http://www.thepublicvoice.org/events/dubai01/presentations/html/a_motaal/motaalpaper.html). The United States has taken the approach that the evolution of technology does not require new legislative texts to protect privacy. See Robert W. Hahn & Anne Layne-Farrar, *Is More Government Regulation Needed to Promote E-Commerce*, 35 CONN. L.REV. 195 (2002); George et al., *supra* note 30, at 746-48. See also LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

<sup>52</sup> See George et al., *supra* note 30, at 746-48. Despite the existence of a legal arsenal of U.S. privacy and judicial decisions, there is a fundamental difference between the EU/Canadian approach to privacy and the U.S. approach to privacy that relates to the definition of privacy used in the respective legal systems. This fundamental difference in the way "privacy" is defined helps explain why privacy tort theories in the United States do not generally protect personal information. U.S. privacy tort law generally protects as "private" only what a reasonable person would view as private. Lin, *supra* note 18, at 1109-12 (explaining why U.S. privacy tort law theories do not adequately protect personal information in the context of electronic databases and the Internet). Such a definition of privacy excludes personal information that relates to an individual that the individual has disclosed to others. *Id.* Under the U.S. viewpoint of privacy, which turns on what a reasonable person would expect to be private and provides a remedy only for highly offensive invasions of privacy, many forms of personal information simply are not "private." *Id.* For example, individuals regularly disclose their personal information to others in employment and other business contexts where the individual either is aware of, could foresee, or even consents to personal data collection. *Id.* Hence, under U.S. tort law, a reasonable person would not expect privacy in personal information that the individual has disclosed to others. *Id.* In other cases, subsequent disclosure and use of the personal information is not highly offensive to a reasonable person, so there is no tort violation. *Id.*

<sup>53</sup> See Lin, *supra* note 18, at 1091-92 ("The notion that computers in general might cause unwanted losses of informational privacy has been well established. . . . [I]nformation, including personal information, is in higher demand than ever before. . . . [C]omputer technology . . . [has] result[ed] in the widespread collection and trading of information." (citations omitted)). Cf. David Scheer, *Europe's New High-Tech Role: Playing Privacy Cop to the World; U.S. Companies Run Afoul of EU Laws on Sharing and Collection of Data*, WALL ST. J., Oct. 10, 2003, at A1 (referencing emerging privacy laws inspired by the EU in South America, Australia, New Zealand, and parts of Asia).

<sup>54</sup> See Lin, *supra* note 18, at 1099-1100. Lin's search for a definition of informational privacy begins with *Whalen v. Roe*, the

informational privacy broadly to include personal information processed in the private employment context, including information processed by electronic monitoring technology.<sup>55</sup> In Canada, PIPEDA similarly focuses on personal information and as of January 1, 2004, applies to all businesses that collect, use, or disseminate such information in the course of commercial activity, including activities tied to the employment relationship and likely including employer electronic surveillance activities.<sup>56</sup> In the United States, however, there is no comparable right to informational privacy in personal information.<sup>57</sup> Broad privacy theories found in U.S. tort law apply to the workplace, yet these theories have failed to restrict electronic workplace monitoring.<sup>58</sup> Except in limited circumstances related to employees' disability or health information, existing U.S. privacy legislation does not recognize a privacy interest in employees' personal information.<sup>59</sup> Further, U.S. privacy laws that ostensibly protect the privacy of electronic communications do not adequately protect employees from electronic monitoring in the workplace, because these laws focus only on the content of employee communications and the methods of electronic surveillance.<sup>60</sup> As a result, U.S. employees in the private sector have little privacy protection for personal information gathered by their employers via electronic means.

### B. *The Evolution of Technology*

¶16

The evolution of information technologies has changed both day-to-day working conditions for employees and also the individual and group relationships forged within the work environment.<sup>61</sup> The privacy issues for employees raised by personal use of the Internet and electronic mail (email) mirror the questions raised when the telephone was first installed and switchboard technology facilitated employer wiretapping and eavesdropping.<sup>62</sup> However, telephone monitoring (and even

---

U.S. Supreme Court's leading case on the issue. *Id.* at 1094; *Whalen v. Roe*, 429 U.S. 589, 599-600 (1977) (finding a constitutionally protected interest that has since been characterized as informational privacy, while upholding the constitutionality of a state statute that required all prescriptions of certain classes of drugs be reported to a state department of health). In *Whalen*, the Court held that the statute adequately prevented the risk of public disclosure and that the government had an essential interest in the medical information, even though the statute required the states to report information that included computerized records containing the names and addresses of the drug recipients. 429 U.S. at 600-601.

<sup>55</sup> See generally EU Privacy Directive, *supra* note 38.

<sup>56</sup> See Privacy Legislation Implementation Schedule, available at [http://www.privcom.gc.ca/legislation/02\\_06\\_02a\\_e.asp](http://www.privcom.gc.ca/legislation/02_06_02a_e.asp) (last visited November 8, 2004).

<sup>57</sup> U.S. law contains:

very few specific legislative data privacy safeguards. Most existing legislation does not address employment relationships, but regulates those between business and consumer or citizen and government. The U.S. concept of a legally enforceable "right to privacy" has expanded slowly. Congress has rejected most attempts to pass comprehensive legislation regulating the treatment of personal data by individuals and businesses in the private sector. The courts are likely to rely on clearly established and articulated state common, statutory, or constitutional law in finding a right of privacy. Americans prefer a regime of industry self-regulation without significant government intervention.

George et al., *supra* note 30, at 746-48 (citations omitted).

<sup>58</sup> The privacy tort that is most frequently applied to workplace privacy issues is the tort of intrusion into seclusion, or into employees' private affairs. See Rothstein, *supra* note 29, at 405-06. If an employer intentionally intrudes, physically or otherwise, upon the solitude or seclusion of the employee in his private affairs or concerns, and a reasonable person would find the intrusion was highly offensive, the employee may be able to recover damages for invasion of privacy under tort law. *Id.* Some employees have been successful in workplace privacy law suits that are based on privacy tort theories, in contexts such as employee drug testing, searching employee work areas, and workplace surveillance. See *id.* See also Wines & Fronmueller, *supra* note 24, at 631-39.

<sup>59</sup> For a discussion of U.S. legislation that does protect the privacy of employees' personal medical information, see *infra* notes 234-53 and accompanying text.

<sup>60</sup> For a discussion of U.S. laws that restrict electronic workplace monitoring by protecting the contents of electronic communications and prohibiting some forms of surveillance, see *infra* notes 210-33 and accompanying text.

<sup>61</sup> See IRF Final Report, *supra* note 1, at 7-8.

<sup>62</sup> See *id.* at 8. See also Sandrine Mathon & Jean-Paul Macker of Commission Nationale de l'Informatique et des Libertés (CNIL), *Cyber-Surveillance in the Workplace* 5 (Feb. 5, 2002), available at [http://www.privacyexchange.org/tbdi/EU\\_HR/cnilcybersurv.doc](http://www.privacyexchange.org/tbdi/EU_HR/cnilcybersurv.doc) [hereinafter, *CNIL Report*] (explaining that the use of automatic telephone switchboards enables employers to find out the telephone numbers dialed by an employee on his or her personal extension). In Europe, the number of companies with Internet access is rising. Finland and Sweden have the most companies with internet access with 91% and 90% respectively, of all companies connected to the Internet. Eironline Study, *supra* note 1, at 4. By comparison, the proportion of U.S. employees with access to the Internet appears also to be on the rise. "According to a Gallup poll, 90% of all large companies, 64% of midsize companies and 42% of small businesses use e-mail. Forty million workers correspond via e-mail, and that number is increasing by 20% per year." Edward Hertenstein, *Electronic Monitoring in the Workplace*:

employee video surveillance) is on the "periphery" of the working process.<sup>63</sup> With the increase of new information technologies, a "genuine migration of the technologies has occurred, from the periphery to the very [center] of the work process."<sup>64</sup>

¶17 For many employees, the workplace is the best place for accessing new technologies, particularly the Internet. Employees are likely to use the Internet during working hours for personal purposes and in some cases even expect that use to be private.<sup>65</sup> However, progress in the capabilities of computer technology has increased the employer's ability to monitor the electronic communications of employees in the workplace. The employer's collection of personal data and other information gathered from electronic monitoring enables a professional, intellectual or even psychological profile of the "virtual employee" to be established, often beyond the legitimate needs of the employer.<sup>66</sup>

¶18 The term electronic monitoring is used in this article to encompass three different concepts. First, it includes an employer's use of electronic devices to review and evaluate the performance of employees.<sup>67</sup> For example, an employer may use a computer to retrieve and review an employee's email messages sent to and from customers in order to evaluate the employee's performance as a customer service representative. Second, it includes "electronic surveillance" in the form of an employer's use of electronic devices to observe the actions of employees while employees are not directly performing work tasks, or for a reason other than to measure their work performance.<sup>68</sup> For example, an employer may electronically review an employee's email messages as part of an investigation of a sexual harassment complaint. Electronic surveillance by an employer also includes compliance with a government search warrant seeking an employee's voice mail or email communications on the employer's systems. Third, electronic monitoring includes an employer's use of computer forensics, the recovery and reconstruction of electronic data after deletion, concealment, or attempted destruction of the data.<sup>69</sup> For example, an employer may use specialized software to retrieve email messages related to an investigation of alleged theft of its trade secrets by retrieving and reconstructing email messages sent by an employee (the alleged thief) to someone outside the company.

¶19 There are many ways that employers may use computer technology to monitor the workplace. Employers may monitor employees' use of computer keyboards.<sup>70</sup> For example, computers may be programmed to monitor clerical workers by recording the number of keystrokes per minute, the exact time and location of any errors, the amount of time it takes to complete each task, and the

---

*How Arbitrators Have Ruled*, 52 DISP. RESOL. J. 36, 37 (1997).

<sup>63</sup> CNIL Report, *supra* note 62, at 3.

<sup>64</sup> *Id.* at 3.

<sup>65</sup> See IRF Final Report, *supra* note 1, at 16.

<sup>66</sup> CNIL Report, *supra* note 62, at 5.

<sup>67</sup> Hébert, *supra* note 2 at n.1 (referencing International Labour Office, 12 Conditions of Work Digest, no. 1, Worker's Privacy Part II: Monitoring and Surveillance in the Workplace 12-13 (1993)).

<sup>68</sup> *Id.*

<sup>69</sup> See Leahy, *supra* note 12; see also *Computer Forensics Defined*, at <http://www.forensics-intl.com/def4.html/> (last visited Dec. 12, 2003).

Computer forensics "deals with the application of law to . . . computer science . . . some refer to it as Forensic Computer Science. Computer forensics has also been described as the autopsy of a computer hard disk drive because specialized software tools and techniques are required to analyze the various levels at which computer data is stored after the fact. Computer Forensics deals with the preservation, identification, extraction and documentation of computer evidence. Like any other forensic science, computer forensics involves the use [of] sophisticated technology tools and procedures which must be followed to guarantee the accuracy of the preservation of evidence and the accuracy of results concerning computer evidence processing. Typically, computer forensic tools exist in the form of computer software. Computer forensic specialists guarantee accuracy of evidence processing results through the use of time tested evidence processing procedures and through the use of multiple software tools, developed by separate and independent developers. . . . Computer forensics is used to identify evidence when personal computers are used in the commission of crimes or in the abuse of company policies. Computer forensic tools and procedures are also used to identify computer security weaknesses and the leakage of sensitive computer data." *Id.*

<sup>70</sup> Hébert, *supra* note 2.

length of breaks.<sup>71</sup> Employers may monitor employees' use of telephones by programming computers to count calls, call-backs, messages, unanswered messages, length of time before calls are answered, the number of times a caller is put on hold, the exact length of each call, and the time period between calls.<sup>72</sup> Employers may also monitor employees' drafting of computer documents.<sup>73</sup> For example, computers may monitor the number of drafts of documents and the number of revisions an employee makes for each line of dictation.<sup>74</sup>

¶20 Advancing technologies enhance employer capability to monitor employee use of computer networks and the Internet within the workplace. Software enables employers to secretly, and in real-time, monitor employees' use of networked computers including individual monitoring of each connected computer.<sup>75</sup> Software enables employers to capture the images from an employee's computer screen at random intervals and then compress those images to provide documentation of all computer work.<sup>76</sup> Software also may reveal the online activities of all employees, including web sites visited, the length of the employees' visits, and whether those sites are productive or unproductive.<sup>77</sup> Software enables employers to monitor employees' use of chat rooms, programs run, games played, files used, bytes transferred or downloaded, time spent downloading, and email sent or received.<sup>78</sup> Additionally, software may be used to monitor employees' computer hard-drives to identify pornography, music, or movies that have been downloaded in violation of copyright laws or workplace policies.<sup>79</sup>

¶21 Employers are increasingly recording, reviewing and disclosing employee electronic communications, including email, Internet connections, and computer files.<sup>80</sup> What follows is a description of the current legal regulation of electronic employee monitoring in the EU, the United States, and Canada.

¶22 In understanding the variation between the jurisdictions' regulatory approaches, it is important to make a distinction between the concepts of "personal data" and data that is the "contents" of "electronic communications" that may be captured through electronic monitoring.<sup>81</sup> Essentially, EU

---

<sup>71</sup> *Id.*

<sup>72</sup> *Id.*

<sup>73</sup> *Id.*

<sup>74</sup> *Id.*

<sup>75</sup> Charles E. Frayer, *Employee Privacy and Internet Monitoring: Balancing Workers' Rights and Dignity with Legitimate Management Interests*, 57 BUS. LAW. 857, 858-59 (2002) (describing available Internet monitoring technology including software that gives employers the ability to monitor in total secrecy and provides a real-time view of the activity that is occurring on any connected computer).

<sup>76</sup> Douglas M. Towns, *Legal Issues Involved in Monitoring Employees' Internet and E-Mail Usage* 2 (Jan. 2002), at <http://www.gigalaw.com/articles/2002/towns-2002-01.html> (describing new technological advances that provide employers a number of options in monitoring devices).

<sup>77</sup> Hébert, *supra* note 2.

<sup>78</sup> See *Automatic Identification of Past Internet Activities*, at <http://www.forensics-intl.com/nta.html> (describing IPFilter software) (last visited Nov. 2, 2004).

<sup>79</sup> John Borland, *Tech Firms Target Workplace Downloads*, ZDNET NEWS (Oct. 8, 2002), at <http://zdnet.com.com/2100-1105-961262.html>.

<sup>80</sup> *Software Enables Employers to Monitor Employees' Internet Use*, 7 EMPLOYMENT TESTING: LAW & POL'Y REP. 55 (Apr. 1998) (estimating that over three quarters of major U.S. firms record and review employee communications and activities on the job, including telephone calls, email, Internet connections and computer files). See also 2001 American Management Survey, *Workplace Monitoring & Surveillance*, at <http://www.amanet.org/research/archives.htm> (last visited Oct. 11, 2002) (detailing practices and policies).

<sup>81</sup> See Lin, *supra* note 18, at 1097-98 (citations omitted).

[I]nformational privacy concerns "personal information." In general, this encompasses any information that is identifiable to an individual. This includes both assigned information, such as a name, address, or social security number, and generated information, such as financial or credit card records, medical records, and phone logs. . . . [P]ersonal information [can be] defined as any information, no matter how trivial, that can be traced or linked to an identifiable individual.

See also Paige Norian, *The Struggle to Keep Personal Data Personal: Attempts to Reform Online Privacy and How Congress Should Respond*, 52 CATH. U.L. REV. 803, 809 (2003) (citations omitted).

Privacy advocates suggest that "the right to be let alone" should include a right to "information privacy" for online transactions requesting personally identifiable information. The term "information privacy" is described as the "desire of

and Canadian regulation of personal data will encompass regulation of electronic communications in the workplace.<sup>82</sup> However, regulation of personal data encompasses more than electronic communications; for example, it also covers privacy issues related to electronic databases containing personal data that exist apart from electronic communications in the workplace.<sup>83</sup> In contrast, U.S. regulation of electronic communications in the workplace is limited to regulation of the "contents" of electronic communications,<sup>84</sup> and often excludes regulation of other data associated with electronic communications, which may be described as "addressing" data. For example, an employee's email communication includes the contents of the email message, as well as the data included in the email header, such as information about the sender and the intended recipient(s), and the date the email message was sent.<sup>85</sup> However, regulation of electronic communications does not cover privacy issues related to electronic databases that exist apart from electronic communications – for example personal data about employees that may be contained in application forms, personnel files, etc.<sup>86</sup> Regulation of electronic communications may also include data related to employees' Internet access, including information that resembles the content of an email message.<sup>87</sup>

¶23

As described in this paper, the EU Privacy Directive and Canada's PIPEDA focus on the broad concept of personal data, which may include content and addressing information related to employee workplace communications as well as employer-maintained databases that contain employees' personal information. In contrast, some U.S. laws provide privacy protection only for the contents of employees' electronic communications. Other U.S. laws protect the privacy of personal data, but only in limited contexts that primarily relate to medical and health information. Making the distinction between privacy of personal data and privacy of the contents of electronic communications is critical to the following sections of this paper.

---

individuals to limit the kinds of information that others know about them." Maintaining information privacy is difficult because both the individual and the online information collector claim control of the personal data.

<sup>82</sup> The Electronic Communications Privacy Act defines electronic communications as follows:

[E]lectronic communication" means 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.

18 U.S.C. § 2510 (2003). 18 U.S.C. § 2510 also defines wire and oral communications.

<sup>83</sup> See Norian, *supra* note 80, at 810 (discussing the ability of companies to collect demographic data about Web site users by monitoring Internet browsing patterns and to distribute this information to others).

<sup>84</sup> See Lin, *supra* note 18, at 1114 (explaining that "there is no prohibition [in the ECPA] on revealing the 'circumstances,' as opposed to the content, of a communication").

<sup>85</sup> See Owen S. Kerr, *Internet Surveillance Law After The USA Patriot Act: The Big Brother That Isn't*, 97 NW. U.L. REV. 607, 611-16 (2003) (discussing the distinction between envelope information and content information and its applicability to email and Internet access). Even though the subject line is in the mail header, it is generally recognized as part of the content of a communication rather than addressing information, as it often includes information that relates to the body of the email message. See *id.* at 613.

<sup>86</sup> See George et al., *supra* note 30, at 738.

Illustrations of the employment data that multinational corporate employers routinely collect, maintain, and transfer to their U.S. offices about their employees and that now are subject to the [EU Privacy] Directive's provisions include: name, address, phone numbers (work and home), gender, employee identification number, dependents, work experience, education, e-mail address, pay, benefits, performance, and training.

*Id.*

<sup>87</sup> An appellate court in the United States recently held that interception of personal information that was part of Internet search queries is of the type of content of an electronic communication that the ECPA covers. *In re Pharmatrak, Inc. Privacy Litigation*, 220 F. Supp. 2d 4 (D. Mass. 2002), *rev'd*, 329 F.3d 9 (1st. Cir. 2003), *remanded to* 292 F. Supp. 2d 263 (D. Mass. 2003) (dismissing the case on summary judgment). The appellate court remanded to the district court to determine whether Pharmatrak intended to intercept the contents of electronic communications, a necessary element of an ECPA violation. *Id.* The District Court found there was no evidence that Pharmatrak intentionally intercepted the electronic communications, and dismissed the case. *Id.* Although *Pharmatrak* involved customer monitoring as opposed to employee monitoring, employers monitoring employee Internet access would be wise to view personal information contained in Internet queries as contents of employees' communication covered by the ECPA, rather than mere addressing information that is not covered by the ECPA. For example, an Internet search query containing the key word "breast cancer" arguably reveals a lot about the subject of an employee's Internet search, particularly if it is captured along with personally identifying information about the sender of the query, like the sender's name.

### III. REGULATION OF ELECTRONIC MONITORING OF EMPLOYEES IN THE EUROPEAN UNION

¶24 In Europe, employee privacy is of fundamental significance. Electronic employee monitoring is currently at the forefront of public debate in the EU precisely because of the prominence of employee privacy rights under European law.<sup>88</sup> Europeans recognize that employers have legitimate interests in controlling the functioning of their businesses and defending against illicit actions by employees that cause harm or increase liability.<sup>89</sup> Europeans also consider new technologies a positive development for resource management.<sup>90</sup> However, the EU is very clear that with respect to workplace privacy and electronic monitoring of employees, the employee's human dignity trumps other considerations.<sup>91</sup>

¶25 Recall that Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms guarantees the right to private and family life, home and correspondence.<sup>92</sup> The European Court of Human Rights interprets the protection of "private life" to include the workplace and extends protection of privacy in correspondence to communications from it.<sup>93</sup>

¶26 *Halford v. United Kingdom* is insightful. The case concerned the interception of an employee's telephone calls. Ms. Halford, the employee, alleged the government's interception violated Article 8. The United Kingdom, adopting a familiar tenet of U.S. privacy law, argued the plaintiff had no "reasonable expectation of privacy" in those calls as they were made using telephones provided by the employer.<sup>94</sup> The European Court of Human Rights disagreed, finding telephone calls made from business premises may be covered by the notions of "private life" and "correspondence" within the meaning of Article 8.<sup>95</sup> Halford had no warning her telephone calls could be intercepted and therefore had a reasonable expectation of privacy in those calls.<sup>96</sup>

¶27 Although *Halford* and other, similar cases before the European Court concern government action, the EU appears to believe Article 8 is relevant in a private context. The Article 29 Working Party,<sup>97</sup> an official EU advisory group formed in connection with the EU Privacy Directive, cites

<sup>88</sup> See Eironline Study, *supra* note 1 (discussing the EU's research and reviews behind a planned directive specifically on the subject of employee electronic surveillance).

<sup>89</sup> See Article 29 Working Document on the Surveillance of Electronic Communications in the Workplace, 6 (May 29, 2002), available at [http://europa.eu.int/comm/internal\\_market/privacy/docs/wpdocs/2002/wp55\\_en.pdf](http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp55_en.pdf) [hereinafter, WPD 2002].

<sup>90</sup> See *id.* at 6.

<sup>91</sup> See *id.*

<sup>92</sup> All Member States in the EU are bound by the provisions of this Convention. The Charter of Fundamental Rights of the European Union, signed in Nice in 2000, recognizes the same rights but uses the word "communications" in lieu of "correspondence." Charter of Fundamental Rights of the European Union, art. 7, 2000 O.J. (C 364) 1, 10, available at [http://www.europarl.eu.int/charter/pdf/text\\_en.pdf](http://www.europarl.eu.int/charter/pdf/text_en.pdf).

<sup>93</sup> WPD 2002, *supra* note 89, at 7-8 (citing *Niemitz v. Germany* and *Halford v. United Kingdom*). In *Niemitz v. Germany*, the European Court of Human Rights held

[r]espect 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 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.

*Id.* at 8 (citing 23 Nov. 1992, Series A n 251/B, par. 29). It is likely that the European Court will interpret Article 8 so as to "keep pace with developments in technology." Eironline Study, *supra* note 1, at 3 (citing URSULA KILKELLY, COUNCIL OF EUROPE, HUMAN RIGHTS HANDBOOKS NO. 1, THE RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE: A GUIDE TO THE IMPLEMENTATION OF ARTICLE 8 OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS (2001)).

<sup>94</sup> *Halford v. United Kingdom*, 24 Eur. Ct. H.R. 523, 523 (1997).

<sup>95</sup> *Id.* at 523.

<sup>96</sup> *Id.*

<sup>97</sup> "The Article 29 Working Party is an advisory group composed of representatives of the data protection authorities of the Member States, which acts independently and has the task, inter alia, of examining any question covering the application of national measures adopted under the Privacy Directive in order to contribute to the uniform application of such measures." Art. 29 Data Protection Working Party Opinion on the Processing of Personal Data in the Employment Context, 2 n.1 (Sept. 13, 2001), available at [http://europa.eu.int/comm/internal\\_market/privacy/docs/wpdocs/2001/wp48en.pdf](http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2001/wp48en.pdf) [hereinafter, WPO].

*Halford* and other relevant European Court cases as significant for employers who electronically monitor their employees.<sup>98</sup> The Working Party extracts three principles from the Article 8 jurisprudence that it applies to public and private workplaces:

1. Workers have a legitimate expectation of privacy in the workplace, which is not to be overridden by the fact that workers use communication devices or any other business facilities of the employer. However, the provision of proper information by the employer to the worker may reduce the worker's legitimate expectation of privacy.
2. The general principle of secrecy of correspondence covers communications at the workplace. This is likely to include electronic e-mail and related files attached thereto.
3. Respect for private life also includes to a certain degree the right to establish and develop relationships with other human beings. The fact that such relationships, to a great extent, take place at the workplace puts limits to employer's legitimate need for surveillance measures.<sup>99</sup>

¶28 Workplace privacy law in the EU also derives significantly from data protection law.<sup>100</sup> What follows is a discussion of the most significant data protection law to date, the EU Privacy Directive, and its application to the employment context and, by extension, to electronic monitoring in the workplace.

¶29 There is currently no EU directive that speaks directly to electronic monitoring of employees in the workplace. Employers operating in the EU thus have strained to interpret the Privacy Directive as applicable to electronic monitoring of employees with little assistance from EU authorities, save a few interpretative documents issued by the Article 29 Working Party.<sup>101</sup> Consequently, member states have struggled to understand the parameters of privacy protection established by the Directive in the context of electronic monitoring practices. As noted previously, each member state was required to adopt national privacy law consistent with the Privacy Directive and to institute a national data protection authority to oversee compliance. Like the Directive, each member state's broad-brush national implementation legislation is applicable to the employment relationship and employment practices including electronic monitoring of employees in the workplace. Thus, on both a supranational and national level there is, with rare exception, a void of statutory law that speaks specifically to the issue and its legality in the face of employee privacy rights.

---

<sup>98</sup> WPD 2002, *supra* note 89, at 7-9.

<sup>99</sup> *Id.* at 9.

<sup>100</sup> See e.g., Kesan, *supra* note 23, at 307. In addition to the EU Privacy Directive, and national laws that implement it, many EU member countries have other legislation that protects the privacy of employees and their communications in the workplace. Eironline Study, *supra* note 1, at Table 3. These protections of privacy are found in the Constitutions of the member states or in their workplace-specific laws. *Id.* Workplace-specific laws in EU member countries that protect the privacy of employees' email and Internet communications are found in:

- Labor statutes;
- Labor agreements (which may be national in scope);
- Criminal statutes that protect the secrecy of private email messages (as opposed to business enterprise-related messages) and may require consent for monitoring;
- Civil statutes that apply when an employer has permitted private email and Internet use by employees; and
- Court decisions (including those requiring employers to have issued clear policies or instructions on email and Internet use before disciplining employees for misuse).

*Id.* In some countries, works councils and other employee representative groups may have legal rights to agree or be informed and consulted before new technology including monitoring equipment is introduced in a workplace. *Id.*

<sup>101</sup> There also exists a draft framework for workplace data protection that was issued by the European Commission after consultation with the social partners on the protection of employee privacy under the Privacy Directive. This framework, however, has been rejected in light of an actual proposed directive on the subject of employee electronic monitoring. Eironline Study, *supra* note 1, at 8.

### A. The EU Privacy Directive

¶30 The EU Privacy Directive is an important foundation for workplace privacy in Europe.<sup>102</sup> The Directive applies to the processing of personal data wholly or in part by automatic means. It establishes common rules for the EU to encourage freer flow of personal data within the Union, thus furthering a unified European Market and protecting citizens' right to privacy.<sup>103</sup>

¶31 By the time the Directive passed, most member states had enacted data protection laws. However, the level of protection varied from country to country making it difficult to transfer information across national borders.<sup>104</sup> The EU Privacy Directive was a response to the perceived threat that European countries with highly protective data laws, such as France and Germany, would impose data transfer bans on states with less rigorous standards.<sup>105</sup> The underlying objective of the Directive was to advance the functionality of the internal market by not only preventing such bans, but also facilitating the free movement of information among the member states.<sup>106</sup> The Directive accomplishes this objective by establishing uniform minimum standards of data protection.<sup>107</sup> Thus, the Directive promotes a system that facilitates territorial uniformity while protecting the fundamental human right to privacy as it relates to personal information.<sup>108</sup>

¶32 The Privacy Directive applies to the processing of "personal data," defined as information relating to an identified or identifiable natural person.<sup>109</sup> 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."<sup>110</sup>

¶33 The Directive applies only to the processing of data, not the ownership of it.<sup>111</sup> Processing is broadly defined as "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, . . . use, . . . dissemination, etc."<sup>112</sup> Individuals ("data subjects") are assured

---

<sup>102</sup> The EU Privacy Directive was supplemented in 2002 by Directive 2002/58/EC concerning the processing of personal data and protection of privacy in the electronic communications sector. See Council Directive 2002/58 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, 2002 O.J. (L 201) 37/EC, available at [http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002L0058&model=gui\\_chett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002L0058&model=gui_chett) (last visited Jan. 31, 2004). Article 3 of the Directive explains it is intended to apply to the "processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks" in the EU. *Id.* (Art. 3) at 43. Both the EU's Privacy Directive and its Directive on Privacy and Electronic Communications have been applied to personal data on the Internet, and the Privacy Directive has been applied more recently to electronic monitoring of employees. See e.g., WPO, *supra* note 89.

<sup>103</sup> George et al., *supra* note 30, at 746. The EU Privacy Directive requires each member state to create an independent supervisory authority to monitor the provisions of the Directive implemented into national law. *Id.* at 754. These national independent authorities have a substantial amount of power as they are authorized to block the transmittal of data, prohibit the processing of data, and/or destroy data processed in violation of the national law. *Id.* at 754.

<sup>104</sup> Existing national legislation was largely based on the OECD Guidelines and the 1981 Council of Europe Convention. See *id.* at 745.

<sup>105</sup> Tracie B. Loring, *An Analysis of the Information Privacy Protection Afforded by the European Union and the United States*, 37 TEX. INT'L L.J. 421, 432 (2002).

<sup>106</sup> The EU's intent to prioritize the free flow of data has been noted by some as "ironic" considering the threat the EU Privacy Directive poses to the flow of personal data from the EU to countries with "inadequate" privacy protection such as the United States. See, e.g., Salbu, *supra* note 47, at 668-69. By adopting the Directive, the EU essentially shifted a regional privacy priority to a global one. *Id.*

<sup>107</sup> George et al., *supra* note 30, at 750.

<sup>108</sup> Loring, *supra* note 105, at 432.

<sup>109</sup> EU Privacy Directive, *supra* note 38 (Art. 2(a)).

<sup>110</sup> *Id.* "This limitation means that European companies can freely develop and share demographic databases as in the United States, when they contain only abstract trends and information, and when no data can be associated with a particular person." Salbu, *supra* note 47, at 670.

<sup>111</sup> Loring, *supra* note 105, at 433. The EU Privacy Directive does not apply to processing of personal data in cases concerning public security, defense, and activities related to criminal law, or to processing by a natural person in the course of purely personal or household activities. EU Privacy Directive, *supra* note 38 (Art. 3).

<sup>112</sup> EU Privacy Directive, *supra* note 38 (Art. 2(b)). Processing even includes referring to a person and identifying them on an Internet page. See, e.g., Case C-101/01, Criminal proceedings against Lindqvist, [2004] 1 C.M.L.R. 20 (2003).

certain rights with respect to their personal data while "data controllers" (e.g., public authorities, internet service providers, or employers) are required to follow a number of rules and restrictions with respect to their data processing operations, including disclosing to data subjects the identities of the data controllers, the recipients of data they collect, and the purposes for which the information is being collected.<sup>113</sup>

1. *Application to the Employment Relationship*

¶34 The Privacy Directive has a direct and immediate effect on the human resource operations of employers.<sup>114</sup> Many employment records involve processing personal data covered by the Directive, including application forms and work references; payroll and tax information; social benefits information; sickness records; annual leave records; unpaid leave/special leave records; annual appraisal/assessment records; records relating to promotions, transfers, training, and disciplinary matters; and records related to workplace accidents.<sup>115</sup> Such data can be very sensitive, as can be the manner in which it is processed by the data controller (here the employer or an agent contracted for the purpose).

¶35 In the EU, employees' privacy rights are balanced against the interests of employers when validating the processing of employees' personal data. The EU recognizes that employers have a legitimate interest in processing such data in the context of the employment relationship and normal business operations.<sup>116</sup> The issue, then, is not whether data processing at the workplace is legal *per se*, but rather, "which are the reasons that may justify the collection and further processing of personal data of any given worker?"<sup>117</sup>

¶36 Pursuant to the Privacy Directive, employees have a number of rights with respect to collection of their personal information by employers, including the rights to be informed generally about information collection practices; to access and correct personal information held by the employer; and, in some cases, to actually withhold consent to the collection and processing of data by the employer.<sup>118</sup> If an employee believes his or her rights are being violated, he or she may appeal to the

---

<sup>113</sup> Loring, *supra* note 105, at 433; Salbu, *supra* note 47, at 670. There are eight privacy principles incorporated into the EU Privacy Directive:

- Purpose limitation (providing information may only be collected for a specific purpose, used in ways consistent with that purpose, and stored for no longer than is necessary to accomplish it)
- Data quality (mandating data be kept accurate and up-to-date)
- Data security (including measures to guard against the improper use and disclosure of information, as well as the security of the processing itself)
- Sensitive data (providing special protection for data revealing racial and ethnic origin, political opinions, religious or philosophical beliefs, and processing that reveals health or sex life)
- Transparency (requiring notice to the data subject that information is being collected about him or her, the purposes for which the information will be used, and the identity of the person collecting the information)
- Data Transfer (prohibiting transfer of data to third parties without express consent by the data subject)
- Independent oversight (requiring appointment of an independent supervisory authority to audit data processing systems, examine complaints by data subjects, and enforce sanctions against data processors in violation of the Directive), and
- Individual redress (permitting data subjects to access their personal information and make corrections, and also allowing them to seek recourse against data collectors and processors when there are violations of the Directive).

Loring, *supra* note 105, at 433-34 (citations omitted).

<sup>114</sup> For an extensive overview of the EU Privacy Directive's relevance to the employment context, see George et al., *supra* note 30.

<sup>115</sup> WPO, *supra* note 97, at 2. Although in practice the EU Privacy Directive directly affects human resources operations, within EU circles data privacy is not seen as a social/employment issue. This explains why human resources departments of United States-based multinationals were not ready for the Directive before 1998. See Angela R. Broughton et al., *International Legal Developments in Review: 1998: Business Regulations*, 33 INT'L.LAW. 291 (1999).

<sup>116</sup> WPO, *supra* note 97, at 19.

<sup>117</sup> *Id.*

<sup>118</sup> George et al., *supra* note 30, at 755-59. The issue of "consent" raises many issues for employers. Many EU countries consider consent to be freely given only when the consent is not made a condition of employment and may be withdrawn at any time. *Id.* at 758. Some countries consider the consent to be effective only if agreed to by the employee's union or works council.

appropriate supervisory authority for relief, or may seek damages in a judicial proceeding.<sup>119</sup> Under the Privacy Directive, employers are liable for monetary compensation to employees whose privacy rights are violated.<sup>120</sup> They are also liable for any additional sanctions under relevant national data protection law.<sup>121</sup>

## 2. *Application to Electronic Employee Monitoring*

¶37 There are no EU regulations or directives specifically devoted to electronic employee surveillance.<sup>122</sup> Instead, there are official guidelines issued by the Article 29 Working Party that interpret the Privacy Directive to cover electronic surveillance of some Internet use and confidential email as well as collection and retention of that data by employers.<sup>123</sup>

¶38 The Article 29 Working Party issued its *Opinion on the Processing of Personal Data in the Employment Context* in late 2001 ("2001 Working Opinion")<sup>124</sup> to specifically address application of the Privacy Directive to the employment relationship. With respect to electronic employee monitoring, the 2001 Working Opinion concluded:

Any collection, use or storage of information about workers by electronic means will almost certainly fall within the scope of the data protection legislation. This is also the case of the monitoring of workers' email or Internet access by the employer. *The monitoring of email necessary [sic] involves the processing of personal data.*<sup>125</sup>

¶39 In May 2002, the Working Party issued the *Working Document on the Surveillance of Electronic Communications in the Workplace* ("2002 Working Document") to compliment the 2001 Working Opinion.<sup>126</sup> The 2002 Working Document establishes specific guidelines concerning what constitute legitimate monitoring activities and the acceptable limits of employee surveillance by employers.<sup>127</sup> Together, the 2001 Working Opinion and 2002 Working Document create minimum guidelines for employers to use in designing and implementing electronic monitoring policies for employees in the EU.

¶40 It should be emphasized that while the Privacy Directive and Article 29 Working Party guidelines create the "blueprint" for a single, EU-wide electronic employee monitoring policy, operations in specific member states must adhere to that state's implementing legislation on data privacy as well as any specific regulations on electronic employee monitoring.<sup>128</sup>

¶41 The Working Party recognized many forms of workplace surveillance are available to the employer, but focused on the two most common: monitoring of employees' email and monitoring of their Internet use. Before employer monitoring activity can be considered lawful and justified, the employer must comply with seven fundamental data protection principles: necessity, finality,

---

Additionally, if consent is given at the outset of the employment relationship, it may not be broad enough to cover subsequent data collection, or if the same data is used for multiple purposes, it may be necessary to obtain consent for each use. *Id.*

<sup>119</sup> *Id.* at 755; EU Privacy Directive, *supra* note 38.

<sup>120</sup> EU Privacy Directive, *supra* note 38.

<sup>121</sup> See, e.g., Data Protection Act, 1998, c. 29 (Eng.) [hereinafter DPA].

<sup>122</sup> See Lugaresi, *supra* note 46, at 2; *but cf.* Eironline Study, *supra* note 1 (noting plans to issue directive by 2005).

<sup>123</sup> WPD 2002, *supra* note 89, at 13-19; WPO, *supra* note 97, at 13-14. In August 2001, the European Commission had its first consultation with employers' organizations and workers' representatives regarding the efficacy of the EU Privacy Directive for the employment relationship. Not surprisingly, employers' associations expressed satisfaction with the status quo. That is, employers believe the Directive is broad enough to govern all forms of processing of personal data in the employment context and are content with the requirements of the Directive's provisions. In their view, additional legislation would amount to excessive regulation. Employees' representatives, on the other hand, believe there needs to be further legislation specifically addressing electronic employee monitoring on the EU level while still allowing for flexibility according to national specificities. See Eironline Study, *supra* note 1. After a second round of consultations, the EU Commission decided to go forward with employment-specific rules on data protection and to issue a directive by 2005. *Id.*

<sup>124</sup> WPO, *supra* note 97.

<sup>125</sup> *Id.* at 2.

<sup>126</sup> WPD 2002, *supra* note 89.

<sup>127</sup> *Id.* at 4.

<sup>128</sup> Broughton, et al., *supra* note 115.

transparency, legitimacy, proportionality, data accuracy, and security.<sup>129</sup> These principles parallel the general privacy principles incorporated into the Privacy Directive; however, there are some notable peculiarities in the Working Party's application of them to electronic employee monitoring.

¶42 The necessity principle requires the form of monitoring be "absolutely necessary" for the employer's purpose. If a more traditional and less intrusive means to accomplish that purpose exists, it must be used in lieu of the monitoring activity. For example, the 2002 Working Document states that only in "exceptional" circumstances such as where the employee is suspected of committing a criminal or seriously wrongful act for which the employer may be held vicariously liable is it "necessary" for the employer to monitor the content of employee email.<sup>130</sup> It may, however, monitor for viruses or to guarantee the security of the system.<sup>131</sup>

¶43 The finality principle requires data be collected only for a specific, explicit, and legitimate purpose and not be processed in any way incompatible with that purpose. For example, if monitoring is justified on the basis of security of the system, the employer cannot use the data to track the individual behavior of employees.<sup>132</sup>

¶44 The transparency principle means an employer must be open and clear about its activities.<sup>133</sup> No covert email monitoring is allowed except where allowed under national law in accord with the Privacy Directive.<sup>134</sup> While not expressly requiring a written policy, the transparency rule dictates that employers' monitoring practices be fully and clearly disclosed to all employees subject to the policy, along with the reasons for the monitoring. This principle further requires employers consult with works councils or other worker representatives before introducing any electronic monitoring policy and, where necessary, obtain their consent.<sup>135</sup> Finally, transparency obliges employers to grant employees essentially unfettered access to their personal data to ensure its veracity and, if necessary, correct any inaccuracies.<sup>136</sup>

¶45 Legitimacy means processing of workers' personal data itself must be legitimate as that term is defined in the Privacy Directive. Legitimate processing includes that necessary for compliance with a legal obligation of the employer; necessary for performance of a contract between the employer and worker; or unambiguously consented to by the worker.<sup>137</sup> It is noteworthy that the concept of consent as a way to legitimize employment practices under EU law is not quite as straightforward as under U.S. law, particularly in the employment context, where withholding consent can have immediate negative job consequences.<sup>138</sup> The Working Party has taken the view that where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data, it is misleading if it seeks to legitimize this processing through consent. "Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment."<sup>139</sup> In other words, "if it is not possible for the worker to refuse it is not consent."<sup>140</sup>

<sup>129</sup> WPD 2002, *supra* note 89, at 13-19.

<sup>130</sup> *Id.* at 13-14.

<sup>131</sup> *Id.*

<sup>132</sup> *Id.*

<sup>133</sup> *Id.*

<sup>134</sup> *Id.* Article 13 of the EU Privacy Directive allows member states to adopt legislative measures that restrict the scope of obligations and rights provided in the Directive when necessary to safeguard important public interests such as national security or the prevention, detection, or prosecution of criminal offenses. *Id.* at 14 n.15.

<sup>135</sup> *Id.* at 15.

<sup>136</sup> *Id.* at 16.

<sup>137</sup> See EU Privacy Directive, *supra* note 38 (Arts. 7(c), (b), (a)). The EU Privacy Directive includes consent as an exception to the prerequisites for processing of personal data where no other exception is applicable. See, e.g., *id.* Arts. 7(a) and 8(2)(a). The Directive defines consent 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." *Id.* Art. 2(h).

<sup>138</sup> The United States considers control of employee privacy a "managerial prerogative in a non-union workplace" and equates "knowledge of an employer's [privacy] policy with consent to be bound to it." Finkin, *supra* note 17, at 814.

<sup>139</sup> WPO, *supra* note 97, at 3.

¶46 Processing may also be legitimate if necessary to legitimate interests pursued by the employer, "except where such interests are overridden by fundamental rights and freedoms" of the employee.<sup>141</sup> It is under this provision of the Directive that an employer may find support for monitoring employees to enforce workplace policies, for example, to prevent harassment of co-workers, or to protect against trade secret theft at the hands of disgruntled employees.<sup>142</sup>

¶47 The proportionality principle mandates personal data must be adequate, relevant, and not excessive in relation to the purposes for collection and/or further processing.<sup>143</sup> The employer's monitoring policy should be tailored to the type and degree of risk the employer faces.<sup>144</sup> This means automatic and continuous employee email and Internet monitoring is prohibited. Email monitoring should be limited to traffic data and size and type of any attachments, and not extend to the actual content of the messages sent or received.<sup>145</sup>

¶48 Data accuracy mandates all records must be accurate, up to date, and retained for no longer than necessary given the legitimate purposes of the employer. As a benchmark, the Working Party suggests retention of data beyond three months would likely be difficult to justify.<sup>146</sup>

¶49 The security principle requires the employer implement appropriate technical measures at the workplace to guarantee personal data of employees is kept secure. The employer may protect against viruses by using automated scanning of emails and network traffic data.<sup>147</sup>

#### *B. Member State Regulation of Electronic Employee Monitoring*

¶50 Like all EU Directives, the Privacy Directive is not itself a law, but rather a direction to the member states to enact implementing legislation consistent with its privacy protection obligations.<sup>148</sup> Consistent with the Directive's mandate, each member state has either adopted new data protection legislation or amended existing legislation to comply with the Directive.<sup>149</sup> Each member state has also appointed an independent national data protection authority to monitor and supervise application of the national data protection law.<sup>150</sup> At present all member states have data protection

<sup>140</sup> *Id.* at 23.

<sup>141</sup> EU Privacy Directive, *supra* note 39 Art. 7(f).

<sup>142</sup> Article 7(c) may provide similar authorization. It permits processing of personal data if that processing is necessary for compliance with a legal obligation to which the controller, here the employer, is subject. Arguably, if an employer is in a jurisdiction that adopts vicarious liability for employers based on employee wrongdoing, an employer needs to monitor employee behavior to detect or prevent any such wrongdoing (e.g., sexual harassment). *Id.* (Art. 7(c)).

<sup>143</sup> WPD 2002, *supra* note 89, at 17.

<sup>144</sup> *Id.*

<sup>145</sup> *Id.* at 18. Note the privacy concern for third-party recipients or senders that may not be aware they are being monitored in connection with the employer's policy.

<sup>146</sup> *Id.*

<sup>147</sup> *Id.*

<sup>148</sup> "A Directive is a piece of European legislation which is addressed to Member States. Once such legislation is passed at the European level, each Member State must ensure that it is effectively applied in their legal system. The Directive prescribes an end result. The form and methods of the application is a matter for each Member State to decide for itself. In principle, a Directive takes effect through national implementing measures (national legislation). However, it is possible that even where a Member State has not yet implemented a Directive some of its provisions could have direct effect. This means that if a Directive confers direct rights to individuals, then individuals could rely on the directive before a judge without having to wait for national legislation to implement it. Furthermore, if the individuals feel that losses have been incurred because national authorities failed to implement [the] directive correctly, then they may be able to sue for damages. Such damages can only be obtained in national courts." EUROPEAN COMMISSION, INTERNAL MARKETS DG, DATA PROTECTION DEPT., DATA PROTECTION IN THE EUROPEAN UNION 4, *available at* [http://europa.eu.int/comm/internal\\_market/privacy/docs/guide/guide-ukingdom\\_en.pdf](http://europa.eu.int/comm/internal_market/privacy/docs/guide/guide-ukingdom_en.pdf) (last visited June 28, 2004) (emphasis omitted).

<sup>149</sup> Member states were required to implement the EU Privacy Directive by 1998. Most of the states did not meet this deadline and the EU Commission in some cases threatened prosecution for the slackers. EUROPEAN COMMISSION, INTERNAL MARKETS DG, DATA PROTECTION DEPT., STATUS OF IMPLEMENTATION OF DIRECTIVE 95/46 ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, *available at* [http://europa.eu.int/comm/internal\\_market/privacy/law/implementation\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/law/implementation_en.htm) (last visited June 28, 2004) (updates on the status of member state implementing legislation); *see also* Eironline Study, *supra* note 1, at Table 3.

<sup>150</sup> EU Privacy Directive, *supra* note 39 (Art. 28). The national data protection authorities have a range of powers with respect to the country's data protection legislation, including: (1) consultation power related to administrative regulations; (2) investigatory

legislation; however, it is rare to find specific legislation applying data protection rules to the employment context.<sup>151</sup>

¶51 When implementing an electronic surveillance policy in the workplace, an employer must adhere to the privacy regulations in each member state in which it is subject to enforcement jurisdiction. This includes national laws regulating privacy and data protection relevant to the workplace, including constitutional provisions and national and provincial or regional legislation that implements the Privacy Directive.<sup>152</sup>

¶52 Beyond enacting legislation to implement the Privacy Directive, member states have begun to issue administrative guidance and executive orders and, in some rare cases, to legislate the employee's right to privacy with respect to electronic monitoring.<sup>153</sup> Belgium is a notable example of a country that has taken a proactive approach to clarifying the relationship between employees' privacy rights and employers' legitimate interests in monitoring employee electronic communications on employer-owned systems. In 2002, Belgian employer and employee representatives signed National Collective Agreement No. 81 on the protection of workers' privacy with respect to controls on electronic online communication data.<sup>154</sup> Royal decree declared the Agreement mandatory for the private sector to govern the employee's right to privacy when electronic communications data are collected for monitoring.<sup>155</sup> The terms of Collective Agreement No. 81 provide reasons that justify employee monitoring, the type of monitoring an employer may conduct, and legitimate procedures for collecting and controlling data. Legitimate justifications for monitoring include prevention of illegal or defamatory acts that can damage the dignity of another person; protection of the employer's economic, commercial, or financial interests; security and effective operation of the company's network systems; and compliance with workplace policies.<sup>156</sup> Collection of data regarding Internet site visits and the number and volume of email messages sent is sanctioned so long as the employee who made the visits or sent the messages is not identified. Clear wrongdoing must be suspected before any type of individualized monitoring is permissible.<sup>157</sup> Finally, in most instances an employee must consent to employer monitoring. Consent must also be obtained from the employee's works council or trade union before any electronic data may be processed.<sup>158</sup>

---

power necessary for performance of their duties; (3) intervention power to block or destroy data processed in violation of data protection law; (4) power to engage in legal proceedings, including calling violations to the attention of judicial authorities; and (5) dispute resolution power to hear claims brought by or on behalf of individuals concerning the protection of their rights in regard to the processing of personal data. Eironline Study, *supra* note 1. See also European Commission, Internal Markets DG, Data Protection Dept., National Data Protection Commissioners, *available at* [http://europa.eu.int/comm/internal\\_market/privacy/links\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/links_en.htm) (last visited June 28, 2004) (listing national data protection commissioners and their contact information).

<sup>151</sup> Eironline Study, *supra* note 1 (noting legislation in Finland, France, Greece, and Portugal). Finland's Act on Data Protection in Working Life, (477/2001) (Fin.) (*available in English at* <http://mol.fi/english/working/dataprotection.html>), is most notable.

<sup>152</sup> There are additional workplace-specific laws in each of the member states that limit electronic monitoring in the workplace, for example, labor laws. See Eironline Study, *supra* note 1, at Table 3 (comprehensive list). An analysis of the complex relationship between these laws and the regulation of electronic employee monitoring is beyond the scope of this paper.

<sup>153</sup> See ELECTRONIC PRIVACY INFORMATION CENTER, PRIVACY AND HUMAN RIGHTS 2002: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS [hereinafter EPIC Report]. Denmark and Germany also have legal provisions that deal with employee email and Internet use and monitoring. Eironline Study, *supra* note 1. In Germany, the Telecommunications Act (TKG) and the Teleservices Data Protection Act (TDDSG) apply when an employer has permitted private email and Internet use by employees. In that case, the employer is more restricted in how it monitors those private communications. Generally, the collection and use of data is permitted for accounting purposes and to ensure system workability. It is generally not permitted to monitor content of personal communications unless there is a clear suspicion of a serious criminal offense. *Id.* Finland and Sweden are also considering legislation on employee privacy in the workplace. *Id.*

<sup>154</sup> *Id.*

<sup>155</sup> *Id.*

<sup>156</sup> *Id.*

<sup>157</sup> *Id.*

<sup>158</sup> *Id.* It is possible an employee representative body may actually consent to a type of electronic monitoring on behalf of employees, such as interception, that violates other law. For example, the Eironline Study notes that the Penal Code in Belgium requires consent by all participants to the communications (not just the employee participant) before an interception may be lawfully made. *Id.* This conflict of laws is representative of the tension that can exist on a national level between privacy law, labor law, and criminal law.

¶53 Adding to the texture of privacy rights inspired by the Privacy Directive, courts in many member states have recently issued rulings with respect to employee privacy rights in the context of electronic monitoring. Most of these decisions involve cases where an employee discharged for violating an employer's electronic system policy (such as an email or Internet use policy) challenges the validity of his or her dismissal as a breach of relevant data protection law. The decisions vary, with some courts approving employee electronic surveillance and others clearly disapproving, particularly where the employee's electronic communications are of a "personal" nature. For example, the Cour de Cassation (the Supreme Court of France) held in *Onof v. Nikon* (2001) that:

The employee has the right, even during working hours and at his workplace, to the respect of his privacy; this includes in particular the confidentiality of his correspondence; the employer cannot, without infringing this fundamental liberty, examine the personal messages sent or received by the employee on a computer tool placed at his disposal for work, and this even in the case of the employer having prohibited a non-professional use of the computer.<sup>159</sup>

¶54 In that case, Frederic Onof, an employee of Nikon France, was suspected of using work time for personal pursuits in violation of company policy. Nikon retrieved and read his stored email files marked "personal," and upon confirming its suspicion dismissed Onof.<sup>160</sup> Onof challenged his dismissal under French wrongful dismissal law and Nikon sought to enter into evidence Onof's email records in support of its decision.<sup>161</sup> The lower courts held the evidence admissible based on their conclusion that there is no greater legal bar in France to employer email monitoring of company systems than in the United States.<sup>162</sup> The French Supreme Court strongly disagreed, basing its decision on Article 8 of the European Convention on Human Rights, Article L 120-2 of the French Labor Code, and Section 9 of the French Civil Code (providing that "[e]veryone has the right to respect for his private life"<sup>163</sup>). It held the employer is not permitted to read employee email and that "doing so is a violation of the fundamental right of secrecy in one's private correspondence even when that correspondence is conducted via an employer's e-mail system and in violation of company policy."<sup>164</sup>

¶55 Two recent German cases on employee privacy suggested that German employers may retrieve an employee's personal electronic communications only if in furtherance of a valid business interest, the employee has been given notice, and the rules governing Internet connection and email use applied by the employer have been agreed to by the employee's elected works council.<sup>165</sup> Furthermore, if an employer in Germany wishes to dismiss an employee for violation of a council-approved employee electronic monitoring policy, it must first give the employee a formal warning. The Regional Labor Court of Hessen recently upheld a lower labor court decision holding an employer is not entitled to dismiss an employee for sending private emails, even where such behavior was expressly prohibited, without a prior formal warning for the infringement. A general warning to

---

<sup>159</sup> *Onof v. Nikon*, Arret No. 4164 (Fr. Oct. 2, 2001).

<sup>160</sup> See Finkin, *supra* note 17, at 813.

<sup>161</sup> France recognizes a cause of action for wrongful or abusive discharge. The principle of "abus de droit" or employer abuse of its rights was adopted by statute in France in 1928. The principle has been interpreted by courts in France to carve out significant exceptions to the rule of employment-at-will. For example, pregnancy, illness, engaging in lawful strike, participation in employee organizations, political beliefs, personal like or dislike, and exercise of citizenship rights no longer form the basis for a lawful dismissal. Plasencia, *supra* note 30, at 299-300. French courts appear to be more willing than American courts to find an employer's dismissal to be wrongful or capricious. *Id.* at 300. Also, French labor law protects against arbitrary dismissal under Title II of the Labor Code. *Id.* at 302.

<sup>162</sup> *Onof v. Nikon*, Arret No. 4164 (Fr. Oct. 2, 2001).

<sup>163</sup> Finkin, *supra* note 17, at 814 (quoting C. CIV. § 9 (Fr)).

<sup>164</sup> *Id.*

<sup>165</sup> *Id.* at 816 (discussing Arb G Hannover, Urt. V. 1.12.2000, 1 Ca 504/100B, reported in NZA 1022 (2001) and Arb G Dusseldorf, Urt. V. 1.8.2001, 4 Ca 3437/01, reported in NZA 1386 (2001)).

all employees that the system may not be used for private use is insufficient to uphold a dismissal on the basis of violation.<sup>166</sup>

¶56 In contrast to the favorable treatment employees appear to receive in France and Germany, the Catalonian High Court in Spain ruled that "an employer was entitled to dismiss an employee who was connected to an Internet game website during working hours for an average of 2-3 hours a day."<sup>167</sup> Even though the employer monitored the employee's computer use covertly, the court held the employee's right to privacy was not infringed. In Spain, secret monitoring is justified where the employer has reasonable grounds to believe the employee is breaching his or her obligations, the surveillance is made over a company computer, and it does not involve accessing the employee's private computer or password.<sup>168</sup>

¶57 An employment tribunal in the United Kingdom reached a favorable holding for employers in the case of *Miseroy v. Barclaycard* (2003).<sup>169</sup> In that case, the employer, Barclaycard, had an employee electronic monitoring policy that was duly disclosed to employees, who were warned the company monitored the computer system for excessive and inappropriate email use and Internet access. During routine monitoring, Barclaycard discovered 900 personal email messages stored on Hilary Miseroy's computer and thereafter investigated the content of the messages under the authority of its surveillance policy. Miseroy's employment was terminated due to the content of his email messages, which included insults to co-workers and leaks of confidential information to a competitor. The employment tribunal held the employer acted correctly in its investigation and firing of Miseroy, even though the email messages were of a personal nature.

¶58 Multinational employers interpreting these cases must do so in the context of evolving guidance promulgated by national data protection authorities on the subject of electronic employee monitoring. Given the dearth of specific legislation regulating monitoring, public guidance offered by the national data protection authority on the legality of employee surveillance is a significant resource for employers operating in a member state.<sup>170</sup>

¶59 One example that is noteworthy for its detailed treatment of employee privacy rights and guidance to employers contemplating electronic employee monitoring is found in the United Kingdom. Its data protection authority, the Information Commissioner, has published The Employment Practices Data Protection Code ("U.K. Code"), which includes, as of June 2003, "Part 3, Monitoring at Work."<sup>171</sup> While not *per se* binding on employers, the U.K. Code is intended to guide employers through the process of complying with the United Kingdom's Data Protection

<sup>166</sup> LAG Hessen, Decision of December 13, 2001.

<sup>167</sup> Raquel Flórez, *More on email abuse*, FRESHFIELDS BRUCKHAUS DERINGER EUROPEAN LAB. LAW BULL., Dec. 2001, available at <http://www.freshfields.com/practice/epb/publications/newsletters/labourlaw/2261.pdf> (last visited June 28, 2004).

<sup>168</sup> *Id.*

<sup>169</sup> See *Tribunal backs e-mail policy at Barclaycard*, PERSONNEL TODAY, Mar. 25, 2003, at 2. Critics of this case argue the court's decision is contrary to the recently adopted chapter in the Employment Practices Data Protection Code on employee monitoring. See *id.*

<sup>170</sup> Data protection authorities in the following member states have issued a variety of statements, guidelines, codes, and regulations with respect to the employment relationship and electronic monitoring: the United Kingdom, Greece, Ireland, Denmark, France, and Italy. See Eironline Study, *supra* note 1, at 19.

<sup>171</sup> United Kingdom Information Commissioner, The Employment Practices Data Protection Code: Part 3: Monitoring at Work (2003) at <http://www.informationcommissioner.gov.uk/eventual.aspx?id=437> (last visited Oct. 18, 2004) [hereinafter, the U.K. Code].

Act,<sup>172</sup> which is binding, by offering "good practice recommendations" to employers operating in the United Kingdom.<sup>173</sup>

¶60 The Code recognizes monitoring is a valid component of the employment relationship.<sup>174</sup> It clarifies that employee electronic monitoring is lawful under the Data Protection Act so long as employers follow the guidelines established in the U.K. Code to ensure the right balance between the legitimate interests of employees and the employer.<sup>175</sup> Two general principles cited as important for employers to follow are transparency and proportionality. Employers wishing to electronically monitor their employees must notify employees and any other party to the communication that they are being monitored (transparency) and must eliminate the collection of personal information that is "irrelevant or excessive" to the employment relationship (proportionality).<sup>176</sup>

¶61 Similar to requirements evolving in other member states' regulation of electronic monitoring, in the United Kingdom, if a communication is marked "private" or "personal" it is generally off-limits and not subject to monitoring unless exceptional circumstances exist, such as suspected belief of gross employee misconduct.<sup>177</sup> In fact, one of the specific recommendations with regard to email monitoring is that employers "encourage workers to mark any personal emails as such and encourage them to tell those who write to them to do the same" so that employers know which messages may not be reviewed for content.<sup>178</sup> Similarly, "covert" or secret monitoring is not justified except in very exceptional circumstances, such as where an employer suspects an employee is engaged in criminal activity and notifying the employee would prejudice a proper investigation.<sup>179</sup>

¶62 The U.K. Code notes that consultation with labor or employee representative groups is not mandatory under current U.K. employment law.<sup>180</sup> Moreover, neither the U.K. Code nor the Data Protection Act "requires" employee consent. Instead, the U.K. Code states "there are limitations as to how far consent can be relied on in the employment context to justify the processing of personal data."<sup>181</sup> Like its sister states in the EU, the United Kingdom seems to question whether consent can

---

<sup>172</sup> Enforcement action would be based on a failure to meet the requirements of the Data Protection Act, not the U.K. Code. However, parts of the Code are likely to be cited by the Information Commissioner in connection with any enforcement action that arises in relation to processing of personal information in the employment context. *See id.* at 6. If a complaint is made to the Information Commissioner, an assessment is made of the alleged offender's data protection practices. *See* DPA, *supra* note 121. Violations of the DPA may result in civil damages to the individual (here the employee) harmed by the data controller's non-compliance, injunctions issued by either a court or the Information Commissioner ordering rectification, blocking, erasure or destruction of data, and ultimately, criminal sanctions (i.e., fines). *Id.* § 60. Directors and officers of corporate data controllers and processors may be found individually liable. *Id.* § 61.

<sup>173</sup> The Information Commissioner promises the benefits to the employer of following the Code's recommendations will be readily apparent. They include increased trust in the workplace, protecting organizations from legal action by employees who might otherwise challenge the employer's data protection policies, consistency with other U.K. laws such as the Human Rights Act, and assisting global businesses to adopt policies that are consistent with similar legislation in other EU countries, thus allowing for integration of the regional privacy effort. U.K. Code, *supra* note 171, at 4.

<sup>174</sup> *Id.* at 12. Note that acceptable methods of employee monitoring do not include interception of electronic communications. It is unlawful to intercept employee electronic communications under the Regulation of Investigatory Powers Act 2000 ("RIPA") and the Telecommunications Regulations 2000. There are exceptions (e.g., interception authorized by warrant), but most of them are inapplicable to monitoring of communications by employers. UNITED KINGDOM INFORMATION COMMISSIONER, THE EMPLOYMENT PRACTICES DATA PROTECTION CODE: PART 3: MONITORING AT WORK, SUPPLEMENTARY GUIDANCE (2003), 28-34, at <http://ico-cms.amaze.co.uk/DocumentUploads/110603supguide.pdf> (last visited Oct. 18, 2004) [hereinafter U.K. CODE SUPPLEMENTARY GUIDANCE]. Even if an exception applies to permit interception, the collection, storage and use of personal information that is involved in the monitoring must still satisfy the DPA. *See id.* at 29.

<sup>175</sup> U.K. Code, *supra* note 171, at 15.

<sup>176</sup> *Id.*; U.K. CODE SUPPLEMENTARY GUIDANCE, *supra* note 174.

<sup>177</sup> U.K. Code, *supra* note 171, at 33. However, in the case of *Misery v. Barclaycard*, the employee email monitored was "personal." The court's ruling in favor of electronic monitoring seems to contradict the U.K. Code's requirements and gives employers the go-ahead to monitor content even in the absence of exceptional circumstances. *See Worker sacked over e-mail*, BBC NEWS (U.K. Edition) (Mar. 18, 2003), at <http://news.bbc.co.uk/1/hi/england/2862353.stm> (last visited Oct. 18, 2004).

<sup>178</sup> U.K. Code, *supra* note 171, at 33.

<sup>179</sup> *See id.* at 37. There are additional recommendations for covert monitoring including requirements that authorization for such monitoring come from senior management, that monitoring be strictly limited to obtaining evidence relevant to the investigation, and that irrelevant evidence be destroyed. *Id.* at 37-38.

<sup>180</sup> *Id.* at 23.

<sup>181</sup> *Id.* at 19.

ever be freely given in the employment context, where a negative job determination for refusal to consent inevitably looms overhead.<sup>182</sup>

¶63 Under the guidelines in the U.K. Code, any adverse impact on individuals that might result from electronic monitoring must be justified by the benefits to the employer and others. The process of determining whether a monitoring arrangement is "justified" is called an "impact assessment."<sup>183</sup> Completing an impact assessment as described in the U.K. Code will help an employer determine if and how to carry out monitoring.<sup>184</sup> The process allows the employer to determine if a monitoring arrangement is a proportionate response to a perceived problem, such as a decrease in worker productivity.<sup>185</sup> Essentially, the impact assessment helps the employer identify and give appropriate weight to the factors it needs to account for in designing an electronic monitoring policy.<sup>186</sup>

¶64 Notably, national data authorities such as the United Kingdom's Information Commissioner are taking it upon themselves to issue guidance for employers on adopting electronic employee monitoring practices. This is surely an attempt to assuage employers who conduct revenue-generating businesses in the United States, but also to protect employee dignity consistent with the values enshrined in European human rights treaties and national constitutions. In the absence of a more specific directive at the EU level and related, consistent national implementing legislation, employers in the EU will rely on varying court interpretations of existing privacy legislation related to personal data privacy. This leaves employers in the EU in a precarious position not completely unlike that of employers in the United States, who face a similar statutory void when it comes to direction on how to protect employee privacy rights while satisfying legitimate business needs.

#### IV. REGULATION OF ELECTRONIC MONITORING OF EMPLOYEES IN THE UNITED STATES

¶65 Lower courts in the United States have had recent occasion to hear cases involving an employer's electronic monitoring of an employee's email communications at work. These cases usually concern

<sup>182</sup> Italy has recently taken a novel approach to the consent issue. Legislative Decree n. 467/2001 (effective Feb. 1, 2002) amended Italian data protection law to eradicate the consent requirement where the data controller (i.e., the employer) "has a legitimate interest in the processing and the rights, freedoms, dignity or legitimate interests of the data subjects [i.e., the employee] do not supercede that interest." *Changes to Data Protection Law*, FRESHFIELD BRUCKHAUS DERINGER INTERNATIONAL IT AND NEW MEDIA UPDATE, Spring 2002, at 3, at <http://www.freshfields.com/practice/ipit/publications/newsletters/ip-update/2855.pdf>. Additionally, the data controller must notify the Garante (the national data protection authority) only of those "processing activities capable of affecting rights and freedoms of the data subjects." *Id.* This includes data that is transferred to non-EU countries. The Garante was charged with issuing specific regulations to help data controllers determine under what conditions processing affects the rights and interests of data subjects. *Id.*

<sup>183</sup> U.K. Code, *supra* note 171, at 15-18.

<sup>184</sup> *Id.* at 15.

<sup>185</sup> *Id.*

<sup>186</sup> *Id.* Impact assessment involves:

- identifying clearly the purpose(s) behind the monitoring arrangement and the benefits it is likely to deliver [such as preventing employee theft of trade secrets];
- identifying any likely adverse impact of the monitoring arrangement [such as intrusion into the private lives of employees, or the effect on employee morale];
- considering alternatives to monitoring or different ways in which it might be carried out [such as investigation based on a specific allegation of employee misconduct rather than continuous monitoring];
- taking into account the obligations that arise from monitoring [such as the cost of keeping collected data secure]; and
- judging whether the monitoring is justified [on the basis of the previous factors and other considerations such as the results of any consultation with trade unions or other representatives].

*Id.* at 16-18. Most employers can complete an impact assessment relatively quickly, at least up until the last step when they have to ultimately resolve if the electronic monitoring policy is justified. The impact assessment model is unique in EU electronic employee monitoring regulation. While adhering to the ideal protections of individual privacy inherent in the EU Privacy Directive and the national implementing legislation, the model at least appears remarkably practical in its application. To compliment the impact assessment model, the U.K. Code incorporates "good practice recommendations" divided into seven subsections, including managing data protection, monitoring electronic communications, and covert monitoring among others. *Id.* at 20-42. *See also*, U.K. Code Supplementary Guidance, *supra* note 174 (including notes, examples, and frequently asked questions). The U.K. Code itself even suggests data protection features to be included in an electronic monitoring policy should the impact assessment warrant implementation. U.K. Code, *supra* note 171, at 30.

an employee dismissal situation similar to those in the EU noted in Section III. The principle focus of the courts seems to be determination whether the employee plaintiff had a "reasonable expectation of privacy" in the contents of the electronic communications (via email, chat room, or message board) leading to dismissal.<sup>187</sup> This analysis is often conducted under privacy tort theories, although other tort theories, such as intentional infliction of emotional distress, may relate to the employer's subsequent use of the employee personal information obtained by electronic monitoring.<sup>188</sup> Generally, employees do not have a reasonable expectation of privacy where communications are sent using employer-provided computers or systems, or where the communication is sent over a company-controlled email system.<sup>189</sup> In cases where the employer has an email and Internet use policy in place and discloses that company-provided systems are subject to electronic monitoring, the expectation of privacy is decreased significantly.<sup>190</sup> Such a policy notifies employees that electronic monitoring may occur, and courts have held it is not reasonable for employees to expect privacy in email communications made using the employer's email system under such circumstances.<sup>191</sup>

¶66

The U.S. Constitution historically provides little protection for employee privacy in private sector workplaces.<sup>192</sup> This is true because the U.S. Constitution has generally been found to restrict only government intrusions into privacy and therefore is inapplicable to workplace privacy intrusions by private employers and other non-governmental actors.<sup>193</sup> State constitutions have also offered little

<sup>187</sup> U.S. courts have analyzed whether a private-sector employee has a reasonable expectation of privacy in workplace communications under a panoply of legal theories found in tort laws, federal and state statutes, contract law, and labor laws. Nancy J. King, *Electronic Monitoring To Promote National Security Impacts Workplace Privacy*, 15:3 EMP.RESP.RTS. J.127, 130-31 (2003). See also Rothstein, *supra* note 30, at 399-407. Tort laws give employees only limited privacy rights in private sector workplaces. The privacy tort most frequently applied to workplace privacy issues is the tort of intrusion into seclusion or into employees' private affairs. King, *supra*, at 187. If an employer "intentionally intrudes, physically or otherwise, upon the solitude or seclusion of the . . . [employee] in his private affairs or concerns, . . . [and] a reasonable person would find the intrusion was highly offensive," the employee may be able to recover damages for invasion of privacy under civil tort law. *Id.* However, U.S. private sector employees generally have no reasonable expectation of privacy that prevents their employers from engaging in intrusive behavior in the workplace, such as monitoring and other surveillance. *Id.* In the rare cases where employees have been found to have reasonable expectations of privacy in their workplaces, employers still generally win most privacy tort cases. *Id.* Employers win these cases because courts often find the employers' alleged privacy intrusions are not unreasonable. *Id.* Sound business reasons often are found to justify employers' actions viewed by employees as invasions of privacy. *Id.* But see Todd M. Wesche, *Reading Your Every Keystroke: Protecting Employee E-Mail Privacy*, 1 J. HIGH TECH. L. 101, 112 (2002) (citing *Vernars v. Young*, 539 F.2d 966 (3d Cir. 1976)). Wesche discusses the holding in *Vernars v. Young* that a corporate officer violated the tort of intrusion upon seclusion when he opened and read mail addressed to an employee and marked personal, without authorization. *Id.* Wesche argues this case suggests a common law right of privacy in one's personal mail and email would be reasonable, even in the workplace. *Id.*

<sup>188</sup> See *infra* note 188 and accompanying text. See also Gabel and Mansfield, *supra* note 1, at 318-19 (commenting that "[t]echnology may increase the risk of conduct being sufficiently outrageous [to constitute intentional infliction of emotional distress] as that technology evolves and impacts recipients"). For example, an employer's use of electronic communications technology may enable personal information about employees to be disseminated in a widespread manner, such that it becomes sufficiently outrageous to constitute intentional infliction of emotional distress. *Id.*

<sup>189</sup> See, e.g., *McLaren v. Microsoft Corporation*, 1999 WL 339015, 5 (Tex. App. 1999) (unpublished opinion). Microsoft won a privacy tort case when it read an employee's email messages stored in personal folders on Microsoft's computer system under a password created by the employee. *Id.* at 1. The court rejected the employee's privacy tort claim, holding he had no reasonable expectation of privacy with respect to email messages stored on his office computer and, even if he did, a reasonable person would not consider Microsoft's interception of these communications to be a highly offensive invasion under these circumstances where the employer was investigating a sexual harassment complaint. *Id.* at 5.

<sup>190</sup> *Garrity v. John Hancock Mut. Life. Ins. Co.*, 2002 WL 974676, 1 (D. Mass. 2002). In *Garrity*, the court dismissed employees' claims of invasion of privacy based on their employer's reading of their email on the employer's computer system. *Id.* at 2. The court held the employer's policy prohibited using the employer's email system to send or receive sexually explicit material and the employees had violated the employer's policy by sending and receiving such messages. *Id.* at 1. See also, EPIC Report, *supra* note 153, at 125.

<sup>191</sup> *Garrity*, 2002 WL 974676 at 1.

<sup>192</sup> Lin, *supra* note 19, at 1150. The constitutionally protected right of privacy is derived from the Bill of Rights of the U.S. Constitution. For example, private sector employees have a Fourth Amendment right to be free from unreasonable searches and seizures by the government. U.S. CONST. amends. IV & XIV; *Kyllo v. U.S.*, 533 U.S. 27, 31 (2001). Private sector employees also have a constitutionally protected right of privacy derived from the "penumbra" of other protections found in the Bill of Rights. See Wesche, *supra* note 187, at 102 (citing *Griswold v. Connecticut*, 381 U.S. 479 (1965) (finding a constitutionally protected right of privacy in the "penumbra" of the First, Third, Fifth, Ninth, and Fourteenth Amendments)).

<sup>193</sup> Lin, *supra* note 19, at 1150 ("[T]he federal constitution is firmly entrenched in the concept that constitutional rights apply only against state actors."). See also Shawn C. Helms, *Translating Privacy Values with Technology*, 7 B.U. J. SCI. & TECH. L. 288, 314 (2001); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1435 (2001); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1230 (1998).

legal protection for employees' privacy in private sector workplaces.<sup>194</sup> Even public employees, who have constitutional privacy rights, have had little success in opposing electronic monitoring of their private communications by government employers.<sup>195</sup> Additionally, constitutional privacy rights have not yet been extended to personal information of the type protected under the EU Data Privacy Directive and national implementing legislation.<sup>196</sup>

¶67 A more pragmatic source of potential privacy rights for private sector employees in the United States is contract law.<sup>197</sup> Contract claims can arise from individual employment contracts, collective bargaining agreements, or in some cases employment policies and manuals.<sup>198</sup> If an employer's policy promises employees their workplace electronic communications will be private and then the employer violates its own policy by reading their personal email, employees may be able to successfully sue the employer for damages for breach of an implied employment contract. Although implied contracts have been enforced in employment situations,<sup>199</sup> employees have not prevailed in any reported case that relates to employer monitoring of email or Internet access. One court even disregarded an oral promise of privacy made by an employer, finding the promise created no privacy rights, or even if it did, the employer acted reasonably in the circumstances.<sup>200</sup>

¶68 Private sector employees<sup>201</sup> protected by federal and state labor laws may also have additional privacy rights under labor statutes or collective bargaining agreements.<sup>202</sup> In workplaces where employees are represented by a labor union, employers may be required to bargain with employees' union representatives before introducing a policy regarding employees' use of information technologies.<sup>203</sup> Under the National Labor Relations Act ("NLRA"), an employer's imposition of a new or substantially revised workplace policy that establishes a basis for discipline is a mandatory

---

<sup>194</sup> Only one state, California, has a state constitution that protects employee privacy from employer intrusions in private sector workplaces. CAL. CONST. art. 1, §1. *See also* Porten v. Univ. of San Francisco, 64 Cal. App. 3d 825, 829 (1976) (holding there is a state constitutional right of privacy for public and private employees); Wesche, *supra* note 187, at 109.

<sup>195</sup> Public employees have constitutional rights to privacy under federal or state laws that employees in the private sector generally do not have, including a Fourth Amendment right to be free from unreasonable searches and seizures by the government. O'Connor v. Ortega, 480 U.S. 709, 715 (1987). In *Kelleher v. City of Reading*, 2002 WL 1067442, 1 (E.D. Pa. 2002), a city employee lost a claim for invasion of privacy against the City of Reading for allegedly publicizing her e-mails and other purportedly private information. In *U.S. v. Simmons*, 206 F.3d 392, 396 (4th Cir. 2000), the federal government used electronic monitoring to examine the records of websites visited by a federal employee and then examined files saved on his computer. *U.S. v. Simmons* recognized that public sector employees may have constitutional privacy rights in some circumstances. *Id.* at 398. However, the court held employees did not have a reasonable expectation of privacy in their electronic communications made in the workplace in light of the employer's policy. *Id.* The policy specified the types of data that would be monitored, including email, Internet, and electronic file transfers, and specified the ways in which the data would be retrieved, including audit and inspection. *Id.*

<sup>196</sup> *See* Norian, *supra* note 81, at 809 (commenting that the Supreme Court has yet to extend constitutional rights to privacy to personal information).

<sup>197</sup> *See* Cottone, *supra* note 30 (commenting that contract claims based on an employer's oral promises or employment documents have been upheld, although damages in contract claims are limited to lost compensation).

<sup>198</sup> *Id.*

<sup>199</sup> *Woolley v. Hoffmann-La Roche, Inc.*, 491 A.2d 1257 (N.J. 1985), *modified*, 499 A.2d 515 (N.J. 1985) (holding absent a clear and prominent disclaimer, an implied promise contained in an employment manual that an employee will be fired only for cause was enforceable).

<sup>200</sup> *Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 100 (E.D. Pa. 1996). The employer prevailed in an invasion of privacy case brought by an employee who was terminated for misuse of the employer's email system. *Id.* The employer retrieved and read the employee's personal email, which was found to contain threatening and unprofessional comments. *Id.* at 98. The court found the employee had no claim of invasion of privacy despite promises by the employer that employees' email would remain confidential. *Id.* at 100.

<sup>201</sup> Some employees are not protected by the NLRA. Generally employees are protected by the NLRA when they work for an employer engaging in interstate commerce and are not supervisors, members of management, or confidential employees. National Labor Relations Act, 29 U.S.C. §§151 *et seq.* (2003) [hereinafter NLRA] (§152(3) deals with limits of protection).

<sup>202</sup> *Id.* *See also* Cottone, *supra* note 30, at 1270; Edward Lieber, *Picketing The Information Superhighway: Must Employers Bargain With A Union Over Their E-Mail Policy?*, 1998 ANN. SURV. AM. L., 517, 530 (1998) (concluding if email policy is germane to the work environment and not at the core of entrepreneurial control it is the subject of mandatory bargaining).

<sup>203</sup> *King Soopers, Inc.*, 340 N.L.R.B. No. 75, 12 (2003) (holding employer violated the NLRA by failing to bargain with the union before implementing a policy regarding use of new technology by employees, under which employees could be disciplined). For example, an employer was required to bargain with union representatives over the imposition of new package inspection practices designed to prevent employee theft. *Edgar P. Benjamin Healthcare Center*, 322 N.L.R.B. No. 128, 752 (1996). So, by analogy, an employer may be required to bargain about electronic monitoring practices designed to prevent employee abuse of its computer systems and violations of its email and Internet use policy.

subject of bargaining.<sup>204</sup> Although an employer must bargain with the union over such policies, the NLRA does not require the parties to agree on the terms of the policy.<sup>205</sup> Instead, the NLRA requires the parties to bargain in good faith about the effects of a workplace policy that concerns a mandatory subject of bargaining before the employer may unilaterally impose the policy. But assuming the required bargaining occurs, unions may not block imposition of the policy.<sup>206</sup> Even where employees have no reasonable expectation of privacy in their electronic communications in the workplace, the imposition of electronic monitoring can interfere with employees' rights under the NLRA, and employees may have a right to bargain with the employer about when or how their email is screened.<sup>207</sup> Additionally, even in non-union workplaces, employer surveillance in the form of email or Internet use monitoring may be prohibited as an unfair labor practice if it constitutes unlawful surveillance of employees engaged in protected, concerted behavior.<sup>208</sup>

¶69 Because U.S. tort, contract, labor, and constitutional laws provide so little privacy protection for U.S. employees, federal and state legislation is the primary source of privacy protection for employees' workplace communications. However, existing statutory privacy protections for employees are very limited. There are two primary categories of legislative privacy protection: 1) statutes that protect electronic communications from certain forms of surveillance; and 2) statutes that protect the privacy of certain categories of personal information, primarily medical information.

#### *A. Federal Statutes that Restrict Forms of Surveillance*

¶70 Federal and state statutes protecting electronic communications from surveillance are often grounded in dated wiretapping laws whose focus is on certain forms of surveillance and whose protections are limited to the contents of electronic communications.<sup>209</sup> In contrast, the EU Privacy Directive and national implementing legislation provide broad protection of personal data, not just the contents of electronic communications, and do not merely prohibit certain forms of surveillance. An examination of the U.S. statutes reveals a weighty focus on determining when there has been an illegal "interception" of communications or an "unauthorized access" to stored communications.<sup>210</sup>

¶71 These statutes also expressly protect only the contents of the electronic communications, not other personal data. The focus on contents of communications in U.S. law leaves much personal data unprotected, such as personal data included in addressing or transactional data related to

<sup>204</sup> King Soopers, Inc., 340 N.L.R.B. No. 75, 12.

<sup>205</sup> Section 8(d) of the National Labor Relations Act (NLRA) defines the duty to bargain as the obligation to "confer in good faith with respect to wages, hours, and the terms and conditions of employment." 29 U.S.C. § 158(d) (2003). The scope of this language sets the boundaries of mandatory bargaining for the employer. JULIUS G. GETMAN, ET AL., LABOR MANAGEMENT RELATIONS AND THE LAW 134-35 (2d ed. 1999). The statutory duty to bargain in good faith requires the parties to bargain until an impasse is reached, which is defined as the point at which the possibility of agreement through continued discussion has been exhausted. *Id.* at 125. At that point, the parties are free to discontinue bargaining. *Id.* Thereafter, the employer may unilaterally implement the terms of the policy that were offered to the union and rejected by it. *Id.* at 126. Refusal to bargain with employees' labor representative or failure to bargain to impasse before unilaterally implementing terms of employment is an unfair labor practice. *Id.* at 117.

<sup>206</sup> Lieber, *supra* note 202, at 554.

<sup>207</sup> *Id.* at 544-545.

<sup>208</sup> Nancy J. King, *Labor Law For Managers Of Non-Union Employees In Traditional and Cyber Workplaces*, 40 AM. BUS. L.J. 827 (2003) (analyzing rights of non-union employees to engage in protected, concerted behavior in workplaces with electronic communications technology including email and Internet access). The right to engage in protected, concerted behavior allows union and non-union employees to discuss matters related to the terms and conditions of their employment and to collectively seek redress of problems related to these matters from their employers. *Id.* at 830.

<sup>209</sup> Peter J. Isajiw, *Workplace E-mail Privacy Concerns: Balancing the Personal Dignity of Employees With the Proprietary Interests of Employers*, 20 TEMP. ENVTL. L. & TECH. J. 73, 81-84 (2001).

<sup>210</sup> However, when U.S. laws prohibit an interception or access, these laws also restrict disclosure of the contents of illegally intercepted or accessed communications. In this way U.S. laws protecting electronic communications from surveillance are similar to the privacy protections under the EU Privacy Directive. In fact, when an interception or an unauthorized access is prohibited by U.S. law, the penalty for a violation may well be much more severe than penalties found under the EU Privacy Directive or national implementing legislation. Criminal sanctions, as well as stiff civil sanctions, are provided for violations of U.S. statutes protecting electronic communications from surveillance.

electronic communications.<sup>211</sup> The focus on contents of electronic communications also leaves uncovered personal data not contained in an electronic communication, such as that in electronic databases of the employer.<sup>212</sup> Additionally, several statutory exceptions are available that courts have found exclude many electronic monitoring activities of employers from coverage under privacy protection statutes.<sup>213</sup> Compared to the extensive regulation of privacy employees enjoy in the EU under the Privacy Directive and national implementing legislation, U.S. employees receive marginal protection of their personal data from the advanced technological tools available to monitor workplace behavior.

¶72 In the United States, the basic federal protection for the privacy of contents of electronic communications is found in the Electronic Communication Privacy Act ("ECPA"), which encompasses federal wiretapping laws and other federal laws prohibiting unauthorized access to communications in electronic storage.<sup>214</sup> Under these federal statutes it is unlawful for anyone, including an employer, to intentionally "intercept" the contents of a wire, oral, or electronic communication ("Title I violations").<sup>215</sup> It is also a federal crime for anyone to "access" without "authorization" a facility providing electronic communication services and thereby obtain access to a wire or electronic communication while it is in electronic storage ("Title II violations").<sup>216</sup>

¶73 Unless the interception or unauthorized access of a wire, oral, or electronic communication is covered by one of several statutory exemptions or defenses, violation of the ECPA is a federal crime. Title I contains exceptions for "business use in the ordinary course of business," "providers of communication systems," and "consent."<sup>217</sup> Title II contains exceptions for "providers of communications" and "authorization by users of communications systems."<sup>218</sup> The ECPA also gives private citizens, including employees, the right to sue for civil damages when there has been an unlawful interception or access to a communication in electronic storage in violation of the privacy rights set out in these statutes.

¶74 The ECPA does not significantly limit employer monitoring in the workplace: "Once an employer meets an exception, the ECPA places no restrictions on the manner and extent of monitoring, nor does it require that an employer notify employees of monitoring."<sup>219</sup> Several

<sup>211</sup> Much personal data is not protected as "contents" of electronic communications. For example, the sender's and receiver's names and e-mail addresses are protected as personal data under the EU Privacy Directive. *See generally* WPD 2002, *supra* note 89, and WPO, *supra* note 97. However, they are not part of the contents of an electronic communication and are therefore not protected from interception or unauthorized access by the ECPA. *See* Lin, *supra* note 19, at 1114.

<sup>212</sup> For example, General Motors Corporation recently found its plan to update its electronic company phone book to include office phone numbers for employees around the world was covered by the EU Privacy Directive because it involved sending the employees' office phone numbers outside the EU. Scheer, *supra* note 53. To comply with the EU Privacy Directive, General Motors Company ("GMC") was required to get the approval of the government privacy agency in the European countries where its employees worked and to satisfy rigorous personal data transfer rules before issuing the global phone book. *Id.* Among other obligations under the EU Privacy Directive, GMC would be required to make disclosures to employees whose personal data would be included in the phone book and to consult with employees' labor representatives where appropriate. *Id.* There is no reason to believe that employees' e-mail addresses would be treated differently than their office phone numbers, so the EU Directive would apply to global e-mail directories as well.

<sup>213</sup> *See e.g.*, *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457 (5th Cir. 1994).

<sup>214</sup> *Konop v. Hawaiian Airlines*, 302 F.3d 868, 874 (9th Cir. 2002). As the court summarized in *Konop*:

In 1986, Congress passed the Electronic Communications Privacy Act (ECPA), Pub. L. No. 99-508, 100 Stat. 1848, which was intended to afford privacy protection to electronic communications. Title I of the ECPA amended the federal Wiretap Act, which previously addressed only wire and oral communications, to "address the interception of...electronic communications." S. Rep. No. 99-541, at 3 (1986), reprinted in 1986 U.S.C.A.N. 3555, 3557. Title II of the ECPA created the Stored Communications Act (SCA), which was designed to "address access to stored wire and electronic communications and transactional records."

The Wiretap Act and the SCA have been amended by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001).

<sup>215</sup> The Wiretap Act, 18 U.S.C. §§ 2510-2522 (2004).

<sup>216</sup> The Stored Communications Act, 18 U.S.C. §§ 2701-2711 (2003).

<sup>217</sup> *Kesan*, *supra* note 23, at 296.

<sup>218</sup> *Id.*

<sup>219</sup> *Id.* at 299.

commentators have concluded that in view of the breadth of the exceptions under the ECPA and the ability of companies to adopt comprehensive electronic communications policies, it will be difficult for employees to sue their employers under the ECPA for electronic monitoring in the workplace.<sup>220</sup>

¶75 However, a few recent cases illustrate that it is at least possible for an employer to violate the ECPA by monitoring the electronic communications of its employees. In *Fischer v. Mt. Olive Lutheran Church*, an employee's claim that an employer violated Title I of the ECPA by eavesdropping on personal telephone conversations made on a work telephone survived summary judgment.<sup>221</sup> The employee's conversation allegedly contained explicit sexual content that was homosexual in nature.<sup>222</sup> After considering application of the ECPA's business use exception, which would permit the employer's interception of the plaintiff's telephone conversation as long as it was in the "ordinary course of its business," the court refused to dismiss Fischer's Title I claim.<sup>223</sup> In *Fischer*, Judge Barbara Crabb held that under Title I, the employer was required to cease listening to Fischer's telephone call as soon as it determined it was personal.<sup>224</sup> The employer did not have a workplace policy permitting interception of employee telephone calls and other electronic communications, so the "consent" exception to the ECPA was not applicable.<sup>225</sup> By contrast to the case law of several EU member states, there are no U.S. cases that have held an employer must stop reading electronic communications, such as e-mail, when it determines the communications are personal in nature.

¶76 When an employer uses electronic employee monitoring *outside the workplace*, the monitoring may violate the ECPA. Access of an employee's off-site e-mail account not provided by the employer may violate the ECPA.<sup>226</sup> And unauthorized access of an employee's non-public and off-site website without authorization may also violate Title II.<sup>227</sup>

¶77 Several recent federal circuit and district court cases have interpreted the scope of the ECPA narrowly, effectively expanding the ability of employers to monitor electronic communications in the workplace without violating the statute. These cases have held an "interception" of an electronic communication is prohibited under Title I of the ECPA only when it occurs while the communication is in transit.<sup>228</sup> Courts have also narrowed the application of Title II of the ECPA, which prohibits unauthorized access to stored electronic communications. Recent court cases have held unauthorized access to stored electronic communications is only prohibited by federal law when the electronic communication is in *temporary storage prior to delivery to the intended recipient*, while access of

<sup>220</sup> See *id.* (collecting references to other commentators).

<sup>221</sup> *Fischer v. Mt. Olive Lutheran Church*, 207 F. Supp. 2d 914, 922-923 (W.D. Wis. 2002).

<sup>222</sup> *Id.*

<sup>223</sup> The court found the employee's telephone conversation was not in the ordinary course of business because it was not a business call and monitoring a personal call was not justified by valid business concerns. *Fischer*, 207 F. Supp. 2d at 923. The court gave two reasons for its holding. *Id.* First, it was unsure how a private telephone conversation raised safety concerns for church personnel that could justify monitoring an otherwise personal call, however sexually graphic and homosexual in nature it may have been. *Id.* Second, the church might have a legal interest in continuing to listen to the conversation if plaintiff were speaking to a minor due to his job responsibilities as a youth minister; however, it was undisputed that the employer's managers believed that the plaintiff was speaking with an adult. *Id.*

<sup>224</sup> *Id.*

<sup>225</sup> *Id.*

<sup>226</sup> *Id.* at 925-26. In *Fischer*, a computer expert hired by the employer guessed an employee's password and used the employer's computers to access the employee's Hotmail e-mail account. *Id.* The computer expert allegedly printed out the e-mail messages found in the account, including messages that appeared to be from a male lover. *Id.* The court let this claim go to trial because Title II prohibits intentionally accessing the storage of other subscribers without specific authorization to do so. See *id.*

<sup>227</sup> See *Konop v. Hawaiian Airlines*, 302 F.3d 868, 879-80 (9th Cir. 2002). In *Konop*, Hawaiian Airlines argued there was no Title II violation because two employees who were authorized to access Konop's website had authorized its manager to access it using their names. *Id.* Hawaiian Airlines argued this access was consistent with the Title II exception that allows persons who are users of an electronic communication service to authorize a third party to access the electronic communications intended for the user. *Id.* The Ninth Circuit held because the two employees had not accessed Konop's website before they authorized Hawaiian Airlines' manager to do so using their names, they were not "users" who could authorize access. *Id.*

<sup>228</sup> *Id.* at 876-79 (holding Konop's Title I claims were properly dismissed by the lower court because Hawaiian Airlines' access of an employee's private secured website without authorization was not an unlawful interception of an electronic communication while it was in transit); *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994) (holding the employer did not unlawfully intercept electronic communications when it seized a computer containing unread e-mail messages because the seizure of the computer occurred sometime after the transmission of the e-mail messages to the computer).

communications in storage after the communication has been delivered to the intended recipient and then stored is not covered.<sup>229</sup> For example, in *Fraser v. Nationwide Mutual Insurance Co.*, there was no Title II violation because the e-mail Nationwide retrieved from its storage site was in "post-transmission storage," having already been sent by the employee and received by the intended recipient.<sup>230</sup>

¶78

Based on the Title I and Title II cases described above, the ECPA does not appear to prohibit an employer from electronically monitoring employee electronic communications (including e-mail, voice mail, and web communications), at least as long as the employer does not intercept those messages while they are in transit or retrieve them from temporary storage or backup storage before the intended recipient has retrieved the messages. However, if an employer uses electronic monitoring software that permits interception of employees' electronic communications in real-time or monitors employees' communications outside the workplace, there is still a risk it will violate the ECPA.<sup>231</sup> The criminal and civil sanctions for such a violation are much more severe than those found under EU or Canadian law.<sup>232</sup> And nothing in the ECPA insulates electronic workplace monitoring from other federal and state laws that may prohibit or limit electronic workplace monitoring, such as laws protecting the privacy of medical information.

### B. Federal Statutes that Protect the Privacy of Medical Information

¶79

The primary source of federal law that requires employers to protect the privacy of medical information related to employees is the Americans With Disabilities Act of 1990 (ADA).<sup>233</sup> The ADA applies to all private-sector employers with more than 15 employees and prohibits disability discrimination by a covered employer with respect to all employment practices and policies.<sup>234</sup> The ADA's medical confidentiality rules protect all applicants and employees of a covered employer, even if the individual does not have a disability as defined by the ADA.<sup>235</sup> Because the ADA applies to all

<sup>229</sup> *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001).

<sup>230</sup> *Id.*

<sup>231</sup> Software that permits real-time monitoring of employees' electronic communications is available. See Frayer, *supra* note 75, at 858. Recent amendments to the ECPA by the USA PATRIOT Act also limit the privacy protections in electronic communications that are provided by federal privacy statutes. See King, *supra* note 187, at 136-37. See also USA PATRIOT Act, *supra* note 214. In October, 2001, the USA PATRIOT Act amended the federal wiretapping laws and the ECPA, amending both the provisions prohibiting interception of electronic communications (Title I) and provisions restricting access to stored wire and electronic communications (Title II). King, *supra* note 187, at 136-37. On October 26, 2001, President Bush signed the USA PATRIOT Act. *Id.* It has over one thousand sections and 342 pages and outlines the government's response to the events of September 11, 2001. *Id.* The Act gives the government enhanced surveillance powers that may affect every employer and provider of Internet communications. *Id.* Some of the Act's provisions take effect immediately, others must be set out in regulations to be promulgated in the coming months, and some will expire automatically in 2005. *Id.* The USA PATRIOT Act's amendments will increase the obligations of businesses to provide information to law enforcement about their customers as well as their employees. *Id.* However, new obligations by businesses to provide information about their customers are beyond the scope of this paper. See Michael A. Benoit and Elena A. Lovoy, *Recent Federal and State Consumer Financial Privacy Developments*, 57 BUS. LAW. 1209 (2002) (discussing the obligations of financial institutions to comply with the privacy provisions of the Gramm-Leach-Bliley Act and the corresponding Regulation P). The employer's new obligations arising from the USA PATRIOT Act include the possibility of the employer being compelled by the government to produce information about former or current employees, including the contents of employees' electronic communications or personal data. See King, *supra* note 187, at 136. See also Elise M. Bloom et al., *Competing Interests in the Post 9-11 Workplace: The New Line Between Privacy and Safety*, 1317 PLI/CORP. 305 (2002); R. J. Cinquegrana & Richard M. Harper, *The USA PATRIOT ACT: Affects [sic] on American Employers and Businesses*, 46-JUN B.B.J. 10 (2002).

<sup>232</sup> Criminal and civil penalties are provided for violations of the ECPA. See King, *supra* note 187, at 133 for a summary of penalties for violating the ECPA, which includes the possibility of imprisonment of up to five years for a Title I violation and up to two years for a Title II violation.

<sup>233</sup> Americans With Disabilities Act of 1990, 42 U.S.C. §§ 12101 *et seq.* (2003) [hereinafter ADA].

<sup>234</sup> 42 U.S.C. § 12101(5); 42 U.S.C. § 12112(a).

<sup>235</sup> The ADA requires employers to keep information collected about employees' medical conditions including medical history, on separate forms, and in separate confidential medical files. 42 U.S.C. §12112(d)(3). It also prohibits disclosure of confidential medical information except for specific job-related reasons related to making necessary medical restrictions to job duties, making reasonable accommodation, anticipating emergency assistance, or to government investigators. *Id.* See also EEOC Enforcement Guidance: *Disability-Related Inquiries And Medical Examinations of Employees Under the Americans With Disabilities Act, Number 915.002*, U.S. Equal Employment Opportunity Commission, July 27, 2000, nn.13-15, available at <http://www.eeoc.gov/policy/docs/guidance-inquiries.html> (last visited April 1, 2004) [hereinafter EEOC Enforcement Guidance on Disability-Related Inquiries Related to Employees]; *Enforcement Guidance: Preemployment Disability-Related Questions and Medical Examinations Under the Americans with Disabilities Act of 1990*, 8 FEP Manual (BNA) 405:7191 (1995) [hereinafter Preemployment

workplace practices and policies, it applies to the employer's electronic monitoring practices and to workplace policies related to employees' use of e-mail and the Internet.<sup>236</sup> As such, the ADA's protections for employees' personal data in the form of medical information limit an employer's prerogatives related to electronic monitoring of employee's communications.

¶80

The ADA provides comprehensive privacy protections for employees related to personal data when that personal information is in the form of medical information. In this regard the ADA is similar to the EU Privacy Directive that protects employee medical information as a form of personal data.<sup>237</sup> The ADA does this by requiring employers to treat applicants' and employees' medical information as confidential, including obligations to keep the information secure.<sup>238</sup> It also limits collection of employees' medical information by limiting inquiries the employer may make to employees and others that could reveal employees' medical information.<sup>239</sup> Further, the ADA prohibits the employer from using and disclosing employees' medical information except for limited job-related reasons.<sup>240</sup> The ADA's rules related to employee medical information apply even when the medical information is voluntarily provided to the employer by the employee.<sup>241</sup> When an employer uses electronic monitoring to collect information about employees' medical conditions, it must consider whether its monitoring is consistent with the ADA's medical confidentiality rules. For example, if an employer scans an employee's e-mail for information about medical conditions or tracks an employee's use of the Internet at work to capture information about visits to health-related websites, it may violate the ADA's prohibitions on making "disability related inquiries."<sup>242</sup> Certainly, an employer's tracking of an employee's visit to a website providing information about cancer treatment could reveal "disability-related" information.<sup>243</sup> However, if an employer monitors an employee's use of the Internet at work for personal use to determine if the employee is observing the company's business-use only policy of the Internet, this monitoring is probably not a violation of the ADA. The ADA would permit electronic monitoring in this case because it is designed to monitor

---

Questions and Medical Examinations], *available at* <http://www.eeoc.gov/policy/docs/preemp.html>.

<sup>236</sup> 42 U.S.C. § 12112(a).

<sup>237</sup> See EU Privacy Directive, *supra* note 39 (Art. 8).

<sup>238</sup> See 42 U.S.C. § 12112(b)(2); see also *EEOC Enforcement Guidance on Disability-Related Inquiries Related to Employees*, *supra* note 235 and accompanying text.

<sup>239</sup> See *EEOC Enforcement Guidance on Disability-Related Inquiries Related to Employees*, *supra* note 235, n.16. Except when the inquiry is job related, employers are prohibited from asking employees for medical information that constitutes a "disability-related inquiry" or gathered medical information pursuant to a "medical examination." *Id.* Inquiries that are prohibited by the ADA because they are not sufficiently job related include a very broad array of inquiries, such as:

[A]sking an employee whether s/he has (or ever had) a disability or how s/he became disabled or inquiring about the nature or severity of an employee's disability; asking an employee to provide medical documentation regarding his/her disability; asking an employee's co-worker, family member, doctor, or another person about an employee's disability; asking about an employee's genetic information; asking about an employee's prior workers' compensation history; asking an employee whether s/he currently is taking any prescription drugs or medications, whether s/he has taken any such drugs or medications in the past, or monitoring an employee's taking of such drugs or medications; and asking an employee a broad question about his/her impairments that is likely to elicit information about a disability (e.g. What impairments do you have?).

*Id.* § 1. Some medical inquiries are not prohibited by the ADA because they are not "disability-related." *Id.* For example, it is lawful for employers to ask employees about: their general well-being; less serious medical conditions that would not reveal a disability; their ability to perform essential job functions; whether they are using illegal drugs; or when a pregnant employee's baby is due. *Id.*

<sup>240</sup> 42 U.S.C. § 12112(b). In essence the ADA prohibits companies from disclosing information about applicants' and employees' medical conditions, physical or mental impairments, and medical treatments to anyone inside the company or outside the company, except when permitted for specified purposes set out in the ADA. *Id.*

<sup>241</sup> The ADA requires employers to treat any medical information obtained from a disability-related inquiry or medical examination (including medical information from voluntary health or wellness programs, as well as any medical information voluntarily disclosed by an employee, as a confidential medical record. *Id.*; *EEOC Enforcement Guidance on Disability-Related Inquiries Related to Employees*, *supra* note 235, at text accompanying n.9. Employers may share such information only in limited circumstances with supervisors, managers, first aid and safety personnel, and government officials investigating compliance with the ADA. *Id.* at text accompanying n.10.

<sup>242</sup> See *supra* note 239 and accompanying text.

<sup>243</sup> The ADA prohibits employers from treating employees differently based on an actual disability, a record of a disability, or a perception of a disability. 42 U.S.C. § 12102(2). Whether the employee actually has cancer, has had it in the past, or is wrongly believed to have cancer, it would generally violate the ADA to use this information as the basis for an employment decision. *Id.*

compliance with workplace policy, not to obtain information about the employee's medical concerns.<sup>244</sup> Electronic monitoring of employee use of the Internet at work is more likely to pass scrutiny if the employer does not collect individualized information that may reveal a disability.

¶81 Thus, the ADA protects employees' privacy in their personal medical information by restricting the employer's processing of employees' medical information to situations that are job-related. Under the ADA, details of an employee's medical treatment or condition are rarely job-related, and the ADA generally prohibits employers from prying into employees' medical condition beyond assessing the ability to perform job functions, need for accommodation, or need for time away from work. Family medical leave laws also restrict the amount of information that an employer may request from an employee or an employee's doctor to substantiate an employee's leave request, and further require employers to keep confidential an employee's medical reasons for taking family medical leave.<sup>245</sup>

¶82 Health care providers, including self-insured employers who provide medical insurance directly for their employees, also have privacy obligations under the medical confidentiality rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).<sup>246</sup> Administrative rules interpreting that act require privacy for customers of health care providers, including employees covered by their employers' self-insured plans (HIPAA Privacy Regulations).<sup>247</sup> The HIPAA Privacy Regulations apply when a health care provider transmits health care information electronically.<sup>248</sup> Under these regulations, the person whose health information is being transferred (including an employee covered by an employer's self-insured plan) is required to give permission for use or disclosure of health care data unless a statutory exclusion applies.<sup>249</sup> HIPAA affords the employee a right to access and review his or her personal information for accuracy, similar to rights reserved for employees to access and review their personal information under the EU Privacy Directive and national implementing laws.<sup>250</sup> There are civil and criminal penalties for violating HIPAA, but the employee has no private right of action to recover compensation under HIPAA.<sup>251</sup>

¶83 Although their coverage is limited to medical information, these federal statutes provide insight into the American perspective on privacy protections for personal information. They are very similar to the privacy protections for employees' personal data found in the EU and national implementing laws (same statement made above). In some cases, particularly with respect to the ADA, the employees' remedies for a violation are superior to those provided in the EU. For example, under the ADA, employees have a private cause of action for damages and may recover actual damages, compensatory damages for emotional distress, and punitive damages, subject to caps on compensatory and punitive damages.<sup>252</sup>

<sup>244</sup> No reported cases have analyzed an employer's electronic monitoring practices in light of the ADA.

<sup>245</sup> See 29 C.F.R. § 825.306(b)(2004) (limiting the amount of information an employer may request to support a leave request); 29 C.F.R. § 825.500(g) (requiring that records containing medical information be kept in separate confidential medical files and maintained according to confidentiality requirements of the Americans With Disabilities Act). See generally, federal Family and Medical Leave Act of 1993, 29 U.S.C.S. § 2601 *et seq.* (2004).

<sup>246</sup> Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 42 U.S.C.S. § 201.1128C. (2003) [hereinafter HIPAA].

<sup>247</sup> HIPAA Privacy Regulations, Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.102, 164.530 (2003) [hereinafter HIPAA Privacy Regulations].

<sup>248</sup> Carter Manny, *Privacy Protection for Health Information Transferred between the European Union and the U.S.: A Comparison of Legal Frameworks*, 36 BUS. L. REV. 107, 109-110 (2003). The HIPAA privacy rules cover "protected health information" which is defined as individually identifiable health information, excluding education records and employment records held by a covered entity in its role as an employer. *Id.*

<sup>249</sup> *Id.* at 110.

<sup>250</sup> *Id.* at 113-114.

<sup>251</sup> *Id.* at 114.

<sup>252</sup> 42 U.S.C. § 12117(a) (2004). Technically, employees must file a discrimination complaint with the U.S. Equal Employment Opportunity Commission (EEOC) and obtain a right to sue letter before filing a lawsuit under the ADA. *Id.*; 42 U.S.C. § 2000e-5(b) (2004) (requiring the EEOC to investigate complaints of disability discrimination); 42 U.S.C. § 2000e-5(f)(1) (2004) (permitting the filing of a civil action at the conclusion of an investigation when complainant has received notice of the right to file such civil action from the EEOC). The EEOC investigates and conciliates such complaints, and eventually issues right to sue letters to

*C. State Privacy Legislation*

¶84 Although the ECPA sets a minimum level of privacy protection for the contents of electronic communications, including those of employees, state wire-tapping statutes may be more protective of electronic communications privacy rights.<sup>253</sup> For example, Florida’s Security of Communications Act is stricter than the ECPA and prohibits intercepting or disclosing the contents of any electronic communication, including workplace communications, without obtaining the consent of both the sender and the recipient.<sup>254</sup> Additionally, some states have statutes that specifically restrict the employer’s ability to monitor an employee’s email without the employee’s consent.<sup>255</sup> For example, Connecticut has a state statute that prohibits employers from electronically monitoring employees’ email without giving employees prior written notice, except in certain circumstances. One circumstance in which monitoring can occur without notice is when the employer has reasonable grounds to believe an employee has violated the law or engaged in conduct that creates a hostile work environment.<sup>256</sup> California passed a similar law in 2001, but it was vetoed by the governor.<sup>257</sup> At the federal level, bills have been introduced in Congress to restrict employers from monitoring employee email. However, none of these bills has been passed.<sup>258</sup> Even in states with wire-tapping laws or laws restricting electronic monitoring, the employer’s email and Internet use policy may make the employer’s electronic monitoring lawful by providing evidence that the employer has provided the notice or obtained the consent required to comply with these state laws.

¶85 Table 1 presents a summary of federal and state law relevant to electronic monitoring of private sector workplaces in the United States.

Table 1. Summary of U.S. Workplace Privacy Law Relevant to Electronic Monitoring of Private Sector Employees

Source of Law	Summary of Law	Protection for Employees?	Type of Remedy: Civil, Criminal
State Tort Laws	Tort of privacy prohibits unreasonable intrusions into the seclusion of employees. Tort of Intentional Infliction of Emotional Distress may restrict employer’s subsequent use of personal data collected through electronic monitoring.	Yes, but no courts have found electronic workplace monitoring to be privacy violation either because there is no reasonable expectation of privacy or the employer’s intrusion was not highly offensive to a reasonable person.	Tort remedies including civil damages and the possibility of punitive damages. Attorney’s fees are not recoverable.
State Contract Law	Promises by an employer create contractual rights that may be enforced by employees. May be	Courts reluctant to find employer monitoring violates contractual rights of privacy.	Contractual damages in the form of lost employee compensation.

employees who want to pursue their ADA remedies in court. 42 U.S.C. § 2000e-5 (2004).

<sup>253</sup> SUBCOMMITTEE ON 21ST CENTURY COMPETITIVENESS, U.S. GOVERNMENT ACCOUNTING OFFICE EMPLOYEE PRIVACY, COMPUTER-USE MONITORING PRACTICES AND POLICIES OF SELECTED COMPANIES (2002), available at <http://www.gao.gov/new.items/d02717.pdf> (last visited Oct. 29, 2003).

<sup>254</sup> See, e.g., Security of Communications Act, FLA. STAT. § 934.01 *et seq.* (2003). See also DAVID M. SAFON, WORKPLACE PRIVACY, REAL ANSWERS AND PRACTICAL SOLUTIONS, 101\_02 (2000) (collecting references to state laws restricting interception and access to electronic communication and workplace specific laws restricting electronic monitoring).

<sup>255</sup> See LEE BURGUNDER, LEGAL ASPECTS OF MANAGING TECHNOLOGY, 619, n.22 (3d ed. 2004). See also SAFON, *supra* note 254, at 101-02.

<sup>256</sup> See, e.g., Conn. Gen. Stat. § 31-48d (2003). See also SAFON, *supra* note 254, at 101-02.

<sup>257</sup> William R. Corbett, *Waiting for the Labor Law of the Twenty-First Century: Everything Old is New Again*, 23 BERKELEY J. EMP. & LAB. L. 259, 274 n.74 (2002).

<sup>258</sup> *d.* at 273 n.71 (discussing the proposed, but never enacted Notice of Electronic Monitoring Act, H.R. 4908, 107th Cong. (2000)).

	express or implied from employer workplace policies.		Generally no recovery of emotional distress damages, punitive damages, or attorney's fees.
The National Labor Relations Act (NLRA)	Requires an employer to bargain with employees' labor representative before imposing an email or Internet use policy that may result in employee discipline.	Yes, applies to employees represented by a labor union (generally limited to non-supervisory employees).	Administrative remedies including reinstatement and backpay. Administrative orders requiring the employer to bargain about mandatory subjects of bargaining. Employee or Union may file an Unfair Labor Practices Complaint with the NLRB.
The National Labor Relations Act (NLRA)	Prohibits employer surveillance of employees engaged in protected, concerted activity without justification.	Yes, applies to employees whether union or <i>non-union</i> (generally limited to non-supervisory employees).	Same as above.
ECPA (Electronic Communications Privacy Act) – Title I	Prohibits contemporaneous interception of oral, wire or electronic communications while in transit.	Yes, exceptions cover workplace monitoring by a provider of a system in the ordinary course of business or with consent.	Civil damages. Criminal penalties. Employees have a private right of action.
ECPA – Title II	Prohibits access to stored wire or electronic communications while in storage prior to delivery to intended recipient.	Yes, exceptions cover workplace monitoring by a provider of a system or with consent.	Civil Damages. Criminal Penalties. Employees have a private right of action.
The Americans With Disabilities Act (ADA)	Limits processing of employees' medical information; prohibits collection of "disability-related" medical information unless job-related; requires security to protect employees' medical information.	Yes, if employer has at least 15 employees. Applies to all employees whether or not disabled.	Civil Damages including compensatory and punitive damages and attorney's fees. No Criminal Penalties. Employees have a private right of action, but must file an administrative complaint with the EEOC prior to filing a lawsuit. See also state disability laws for possible additional protections.
HIPAA	Requires protection of the privacy of personally identifiable health care information including security protections. Provides rights of access for data subjects.	Yes, if covered by an employer's self-insured health care plan	No private right of action. Civil fines and criminal penalties available in a government enforcement action.
State Electronic Communications Privacy Statutes	Prohibits interception of oral, wire or electronic communications. See specific state laws. May not restrict access to stored communications.	Yes	Civil Damages and/or Criminal penalties -- see state laws. May be no private right of action.
State Statutes Restricting Electronic Monitoring	Individual states may have statutes restricting electronic monitoring by employers or requiring employers to notify	Yes	See state laws.

	employees of electronic monitoring practices.		
--	---	--	--

## V. REGULATION OF ELECTRONIC MONITORING OF EMPLOYEES IN CANADA

¶86 As in the United States, the right to privacy in Canada has constitutional legitimacy and is primarily found in Section 8 of the Charter of Rights and Freedoms of 1982,<sup>259</sup> which guarantees a right to be "free from unreasonable search and seizure."<sup>260</sup> Strictly speaking, the Charter would not apply to the relationship between private parties, such as an employer and employee (unless of course the employer was a Crown corporation or otherwise connected to government).<sup>261</sup> However, the Supreme Court of Canada in several cases has affirmed that while the Charter does not apply to private disputes *per se*, Canadian courts should incorporate Charter values when interpreting other federal or provincial legislation which may be the subject of dispute between private parties.<sup>262</sup> Therefore the Charter, and what may be considered Charter values, will govern any interpretation of privacy rights between private parties, including employers and employees.

¶87 The notion of applying Charter values,<sup>263</sup> particularly the right to be free from unreasonable search and seizure, suggests that a standard of "reasonableness" must be present in any restriction upon an employee's right to privacy. This standard has proven useful in determining the right of a privacy expectation in the workplace. In *R. v. Duarte*, the Supreme Court held that electronic surveillance by the State "is a breach of an individual's right to privacy and will only be countenanced by application of the standard of reasonableness."<sup>264</sup> In *Re Doman Forest Products Ltd. 1990 BC Arbitration*, a British Columbia arbitrator applied the principles in *Duarte* and Charter values stemming from Section 8 jurisprudence to the issue of an employer's surveillance of employees.<sup>265</sup> The arbitrator concluded that the right to employer surveillance must be balanced with the right to privacy and determined by considerations of what is "reasonable in all of the circumstances."<sup>266</sup>

¶88 In these cases, the standard of reasonableness requires a balancing of the right of individual employees "to be left alone" and the right of employers to intrude in furtherance of their legitimate business interests.<sup>267</sup> Unlike the U.S. with its selection of lower court cases on the subject, there are no cases in Canada that define the balancing test in the context of challenging an employer's right to electronically monitor employees in the workplace.<sup>268</sup> Based on existing jurisprudence and scholarly

<sup>259</sup> Can. Const. (Constitution Act, 1982) ch. 11 (Canadian Charter of Rights and Freedoms), § 8. [hereinafter Charter].

<sup>260</sup> Although the Charter applies only to governmental action, judicial interpretation of Section 8 has advanced the understanding of the right to privacy in Canadian jurisprudence in general. There is also a possibility that the section 7 right to "life, liberty and security of the person" can encompass a right to privacy. Tina Piper notes that a number of cases, including *R. v. Morgentaler*, [1988] 1 S.C.R. 30 (Can.), have expanded the section 7 definition of "security" beyond the criminal context of arbitrary detention to include "personal autonomy." Tina Piper, *The Personal Information Protection and Electronic Documents Act: A Last Opportunity to Democratize Canada's Technological Society*, 23 DALHOUSIE L.J. 253, 263 n.44-45. (2000). A.W. MacKay notes that the minority position in *Godbout v. Longueuil*, [1997] 152 D.L.R. (4th) 577 at para. 69, invokes international law in its discussion of privacy issues and its general discussion of the scope of section 7 of the Charter. A.W. MacKay, *The Waves of Information Technology, the Ebbing of Privacy, and the Threat to Human Rights*, 10 N.J.C.L. 411, 422-23 (1999). For other judicial interpretations of Section 7 in terms of privacy, see generally: *B. (R.) v. Children's Aid Society of Metropolitan Toronto*, [1995] 1 S.C.R. 315 (Can.); *Godbout c. Longueuil (Ville)*, [1997] 3 S.C.R. 844 (Can.); *R. v. O'Connor*, [1995] 4 S.C.R. 411 (Can.); *R. v. Jones*, [1986] 2 S.C.R. 284 (Can.); *Singh et al. v. M.E.I.*, [1985] 1 S.C.R. 177 (Can.); *Rodriguez v. B.C.*, [1993] 3 S.C.R. 519 (Can.).

<sup>261</sup> See Charter, *supra* note 229, § 32(1).

<sup>262</sup> See, e.g., *Hill v. Church of Scientology of Toronto*, [1995] 2 S.C.R. 1130 (Can.); *RWDSU v. Dolphin Delivery Ltd.*, [1986] 2 S.C.R. 573 (Can.); *McKinney v. University of Guelph*, [1990] 3 S.C.R. 229 (Can.).

<sup>263</sup> See *Dolphin Delivery*, 2 S.C.R. at pp. 592-93.

<sup>264</sup> *R. v. Duarte*, [1990] 1 S.C.R. 945 at para. 50.

<sup>265</sup> *Re Doman Forest Products Ltd.*, [1990] 3 L.A.C. (B.C.) (4th) 275, at 280.

<sup>266</sup> *Id.*

<sup>267</sup> What constitutes 'reasonableness' was commented upon by La Forest J in *Duarte*: "It [is] necessary to strike a reasonable balance between the right of individuals to be left alone and the right of the state to intrude on privacy in the furtherance of its responsibilities for law enforcement." [1990] 1 S.C.R. 30, at 45.

<sup>268</sup> But see generally *R. v. Weir*, [1998] 59 Alta. L.R. (3d) 319 (QB) *aff'd on appeal* (finding a reasonable expectation of privacy in individual emails using a third party ISP); *Pacific Northwest Herb. Corp. v. Thompson*, [1999] B.C.J. No. 2772 (employee has expectation of privacy in employer-owned computer used at home by the employee for personal reasons). There are also a

interpretations, factors that are considered important in determining the reasonableness of employer electronic surveillance of employees include: (i) whether it was reasonable to request surveillance; (ii) whether the surveillance was conducted in a reasonable manner; and (iii) whether any other alternatives to surveillance were available to the employer. These principles have been frequently referred to in Canadian writing and it seems likely that they would be considered in a judicial interpretation of the right of employers to monitor employee emails and other forms of electronic correspondence.<sup>269</sup>

¶89 What follows is a discussion of how these principles are reflected in federal and provincial privacy legislation, most importantly in Canada's newly enacted Personal Information Protection and Electronic Documents Act (PIPEDA), and how they influence the ability of employers to electronically monitor employees in the Canadian workplace.

#### *A. Federal Privacy Legislation*

¶90 Prior to the adoption of PIPEDA, Canadian privacy legislation provided only a fragmented, piecemeal approach to the protection of workplace privacy not unlike that which currently exists in the United States, and much less comprehensive than that found in the EU. For example, Canada's Privacy Act<sup>270</sup> protects an individual's privacy with respect to government data collection. A number of other laws have been enacted to apply to the collection of personal information in Canada by government-regulated organizations in different sectors.<sup>271</sup> However, none of these statutes appear directly relevant to the issue of whether a private sector employer can monitor employee emails.

¶91 In the criminal arena, Section 184(1) of the Canadian Criminal Code makes it an indictable offence to willfully intercept private communications by "means of any electro-magnetic, acoustic, mechanical or other device."<sup>272</sup> However, this provision does not apply to interception in which a party to the communications has "consented," as is likely to be the case when an employee agrees to an employer's policy on electronic monitoring. Second, unlike the ECPA's prohibitions on access to

---

number of labor arbitrations on wrongful dismissal which are relevant in understanding how far the employee's expectation of privacy reaches and the employer's justification for using electronic evidence of employee wrongdoing to support dismissal. *See, e.g.,* Michael Geist, *Computer and E-Mail Workplace Surveillance in Canada: The Shift from Reasonable Expectation of Privacy to Reasonable Surveillance*, p. 19 at [http://www.cjc-ccm.gc.ca/english/publications/Geist\\_report.en.pdf](http://www.cjc-ccm.gc.ca/english/publications/Geist_report.en.pdf) (last visited Jan. 29, 2004).

<sup>269</sup> For a general overview of the effect of Doman pre-PIPEDA, *see* Diba Majzub, *Employee Privacy: A Critical Examination of the Doman Decision*, 4 Appeal Rev. Current L. and L. Reform 72, (1998). The case of *R. v. Plant*, although a Charter case, is also instructive for understanding the parameter of workplace privacy in Canada. [1993] 3 S.C.R. 281, 294. Sopinka J. established a framework for determining an individual's expectation of privacy in the workplace which included consideration of the following factors: The nature of the information

- The nature of the relationship between the parties and the party claiming its confidentiality
- The place where the information was obtained
- The manner in which it was obtained
- The seriousness of the crime being investigated allowing for a balancing of the societal interests in protecting individual dignity, integrity and autonomy with effective law enforcement.

*Id.* at 293.

<sup>270</sup> Federal Privacy Act, R.S.C. ch. P-21 (1985) (Can.). Many provinces have similar legislation. *See, e.g.,* Freedom of Information and Protection of Privacy Act, R.S.A., ch. F-25 (2000) (Alberta), *available at* <http://www3.gov.ab.ca/foip/> (last visited Jan. 24, 2004); Freedom of Information and Protection of Privacy Act, R.S.B.C., ch. 165 (1996) (British Columbia), *available at* [http://www.msar.gov.bc.ca/FOI\\_POP/Index.htm](http://www.msar.gov.bc.ca/FOI_POP/Index.htm) (last visited Jan. 24, 2004); Freedom of Information and Protection of Privacy Act, C.C.S.M., ch. 175 (1997) (Manitoba), *available at* <http://www.gov.mb.ca/chc/fippa/index.html> (last visited Jan. 24, 2004); Freedom of Information and Protection of Privacy Act, R.S.O., ch. M-56 (1990) (Ontario), *available at* <http://www.gov.on.ca/MBS/english/fip/act/act.html> (last visited Jan. 24, 2004); Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information, L.R.Q., ch. A-2.1 (Quebec), *available at* <http://www.cai.gouv.qc.ca/fra/docu/loiaccs.pdf> (last visited Jan. 24, 2004). English version available at: <http://www.privacyinfo.ca/>. *See* PrivacyInfo.ca, at <http://www.privacyinfo.ca/legi.php?v=6> (last visited Jan. 24, 2004) (exhaustive and up-to-date list of provincial privacy laws).

<sup>271</sup> Such acts included the Bank Act, ch. B-1.01, S.C. 1911 (Can.), the Postal Services Continuation Act, 1997, S.C. 1997, c. 34 (Can.), and the Insurance Companies Act, ch. 47, § 489, S.C. 1991 (Can.). In January 2004, all organizations and private companies became subject to PIPEDA. *See* Privacy Commissioner of Canada, Implementation Schedule, at [http://www.privcom.gc.ca/legislation/02\\_06\\_02a\\_e.asp](http://www.privcom.gc.ca/legislation/02_06_02a_e.asp) (last visited Jan. 31, 2004) [hereinafter PIPEDA Implementation Schedule].

<sup>272</sup> Criminal Code of Canada, R.S.C. 1985, c. C-46, s. 184.2(1).

stored electronic communications, the Canadian prohibition on "interception" does not appear likely to prohibit access to emails which would be stored after transmission, and therefore incapable of being "intercepted" on an employer's system.<sup>273</sup> Thus far, the Criminal Code has not been applied to employer monitoring of employee email.

¶92 Inspired by the EU Privacy Directive, in 2000 Parliament passed PIPEDA, comprehensive legislation to protect privacy rights throughout Canada.<sup>274</sup> To permit harmonization of laws, PIPEDA is being phased-in. Phases 1 and 2 have already taken place, and Phase 3 brought the remaining portions of PIPEDA into force as of January 2004.<sup>275</sup>

¶93 Under Phase 1, which became effective in 2001, PIPEDA covers the collection, use or dissemination of personal information "in the course of commercial activity" by all federally regulated organizations, with the exception of any health information.<sup>276</sup> "Commercial activity" includes "any particular transaction, act, or conduct, or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fund-raising lists."<sup>277</sup> Phase I of PIPEDA also applies to all businesses conducting international or inter-provincial trade, which could therefore include Crown corporations (i.e., federal corporations) working or employing persons internationally. The Privacy Commissioner has stated that Phase I of PIPEDA also applies to "all organizations that disclose personal information for consideration outside a province or the country" in the course of commercial activity, and therefore may include multinational or inter-provincial employers.<sup>278</sup> Phase I of PIPEDA does not cover provincially-regulated commercial activities.

¶94 Under Phase 2, which became effective in 2002, PIPEDA's coverage was expanded to apply to the collection of all personal health information by federally regulated businesses, and those conducting international or inter-provincial trade.<sup>279</sup> Finally, in Phase 3, which became effective on January 1, 2004, PIPEDA's coverage was expanded again to include all businesses, whether federally or provincially regulated or strictly private, and to their collecting, using, or disseminating information "in the course of commercial activity" in Canada.<sup>280</sup> This means that PIPEDA now applies to the personal information collected by all organizations in Canada, whether federally or provincially regulated, as long as the information is being used for commercial activity (i.e., for "profit or gain").<sup>281</sup>

¶95 Like the EU Privacy Directive, PIPEDA does not specifically address the issue of any employer's monitoring of employee electronic communications. However, the stated purpose and scope of PIPEDA suggest that this legislation will govern employer-monitoring scenarios in the private sector, with some exceptions.<sup>282</sup>

---

<sup>273</sup> Compare the definition of "interception" under the ECPA. See *infra* notes 210-212 and accompanying text. For a similar interpretation, see Melanie Samuels and Sara Gregory, *Privacy Issues in the Workplace: Employer Monitoring of Employee Technology Use*, materials prepared for the Continuing Legal Education Society of British Columbia, (May 10, 2001), at <http://www.lawsonlundell.com/resources/PrivacyIssuesWorkplace.pdf>. The authors also importantly point out that an employee who has consented to a privacy policy would thereafter not have a reasonable expectation of privacy. The concept of 'reasonable expectation' of an employee's privacy is discussed *infra*.

<sup>274</sup> Despite the separation of powers between federal and provincial activities in the Canadian Constitution, PIPEDA is legally applicable to privacy issues in both spheres. See *General Motors v. City National Leasing*, [1989] 1 S.C.R. 641 (Can.). For commentary on the passage of PIPEDA and its effects on the business community, see Michael Geist, *Fighting privacy law questionable*, *TORONTO STAR*, Jan. 19, 2004, available at [http://www.thestar.ca/NASApp/cs/ContentServer?pagename=thestar/Layout/Article\\_Type1&call\\_pageid=971358637177&c=Article&cid=1074467408174](http://www.thestar.ca/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&call_pageid=971358637177&c=Article&cid=1074467408174).

<sup>275</sup> PIPEDA, *supra* note 49, § 72.

<sup>276</sup> *Id.* § 30.

<sup>277</sup> *Id.* § 2(1).

<sup>278</sup> See PIPEDA Implementation Schedule, *supra* note 271.

<sup>279</sup> *Id.*

<sup>280</sup> *Id.*

<sup>281</sup> *Id.*

<sup>282</sup> PIPEDA allows provinces to opt out of its application if the province has enacted legislation that is "substantially similar."

¶96 The definition of what constitutes "personal information" covered by PIPEDA is broad and seems likely to encompass employee-generated email and other forms of electronic communication. PIPEDA defines "personal information" as including any information pertaining to an individual including employee files, but does not include the name, title, business address or telephone number of an organization's employee.<sup>283</sup> PIPEDA applies to all personal information collected by an organization in the course of commercial activity.<sup>284</sup> PIPEDA also applies to personal information that "is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business."<sup>285</sup>

¶97 PIPEDA incorporates Charter privacy principles including the requirement for balance between an individual's right to privacy and reasonable collection and use of personal information. The Privacy Commissioner has described PIPEDA as striking "a balance between an individual's right to the protection of personal information and the need of organizations to obtain and handle such information for legitimate business purposes."<sup>286</sup> To accomplish this objective, PIPEDA incorporates the Canadian Standards Association's Model Code for the Protection of Personal Information (the "Model Code").<sup>287</sup> The Model Code found in Schedule 1 of PIPEDA clearly sets out the principles to which organizations must conform prior to collection, use or dissemination of any such information, including:

1. Accountability: every organization will be responsible for personal information it collects, and to this end shall designate an individual(s) (i.e. internal privacy officer) who is responsible for ensuring the organization compliance with the principles listed below (i.e. the organization's accountability).
2. Identifying Purposes: the organization shall specify the purpose for which it is collecting information at or before the time the information is collected.
3. Consent: An individual's knowledge and consent are required for the collection, use or dissemination of information, subject to some exceptions.<sup>288</sup>
4. Limiting Collection: Any personal information which is collected shall be limited to the purpose identified by the organization, and shall be collected using fair and lawful means.
5. Limiting Use, Disclosure, and Retention: collected personal information shall be used only for the purpose it was collected, subject to the exceptions of consent of the individual or as required by law. An organization is entitled to keep information only as long as is necessary to fulfill the stated purpose.
6. Accuracy: collected personal information must be accurate, complete and as timely as

---

So far the Privacy Commissioner has deemed only Quebec's statutes, *infra*, to be substantially similar. The draft legislation currently being pushed through the parliaments of British Columbia and Alberta, and expected to come into force by January 2004, will also be substantially similar. Ontario hopes to pass 'substantially similar' legislation some time in 2004.

<sup>283</sup> PIPEDA, *supra* note 49, § 2(1).

<sup>284</sup> *Id.* § 4(1).

<sup>285</sup> The statute defines an "organization" broadly to include "an association, a partnership, a person, and a trade union." *Id.* § 2.

<sup>286</sup> PRIVACY COMMISSIONER OF CANADA, Background: The Personal Information Protection and Electronic Documents Act (Dec. 2000), at [http://www.privcom.gc.ca/information/02\\_06\\_07\\_e.asp](http://www.privcom.gc.ca/information/02_06_07_e.asp). Note, this concept of 'balancing' appears in line with the case law which has addressed the use of employee's personal information by an employer, *see discussion infra*.

<sup>287</sup> *See* PIPEDA, Schedule 1, Principles set out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96, s. 4.1 to 4.10.4, *available at* <http://canada.justice.gc.ca/en/news/nr/1998/attback2.html> (last visited Jan. 31, 2004) [hereinafter CA Model Code].

<sup>288</sup> Exceptions include information collected to advance law enforcement or journalistic purposes, as follows:

- (i) if obtaining consent would compromise the accuracy of the information being collected;
  - (ii) if obtaining the information clearly benefits the individual;
  - (iii) where the personal information is required pursuant to a legal investigation or to aid in an emergency where people's lives and safety could be at stake;
  - (iv) in an emergency, to assist a legal investigation or conserve historically important records; or
- to collect personal information to be used solely for journalistic, artistic, or literary purposes.

PIPEDA, *supra* note 49, §§ 7(1)(a) - (d), 7(2)(e).

- required for the purposes that it is being used.
7. Safeguards: Security safeguards must be implemented and operated to protect the personal information which is collected.
  8. Openness: an organization must have specific information about its policies and practices regarding the management of personal information in place, and readily available to individuals.
  9. Individual Access: upon request, an individual shall be informed of "the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate."
  10. Challenging Compliance: an individual shall be able to address a challenge concerning compliance with the above principles to the designated person(s) established in (1).<sup>289</sup>

¶100 The Model Code standards are remarkably similar to the EU Privacy Directive's foundation principles and the seven fundamental data protection principles applied by the Working Party to employer electronic surveillance of employees in the EU.<sup>290</sup> One noteworthy difference for employers in Canada is that the Model Code has the force of federal law, unlike the EU Privacy Directive and the Working Party official opinions. Recall that in the EU, it is incumbent on each Member State to provide recourse to employees whose privacy rights are adversely affected by employer electronic surveillance tactics. In contrast, in Canada an employer's non-compliance with PIPEDA Schedule 1 will provide recourse for an individual to the Privacy Commissioner.<sup>291</sup>

¶101 Under PIPEDA, individuals may file a "complaint" with the Privacy Commissioner for any aspect of an organization's compliance with the provisions of PIPEDA's personal information protections.<sup>292</sup> The Privacy Commissioner is empowered to attempt dispute resolution and make recommendations to the respective parties. While non-binding, these recommendations have been shown a degree of consideration and deference by the Federal Court.<sup>293</sup> For example, since the passage of PIPEDA there have been decisions that have focused either on the Privacy Commissioner's scope to investigate complaints, or on a federally regulated organization's use of "personal information" under the act.<sup>294</sup>

<sup>289</sup> See Canada Model Code, *supra* note 287.

<sup>290</sup> See *infra* notes 131-147 and accompanying text.

<sup>291</sup> PIPEDA, *supra* note 49. Section 11 Part (1) states, "[a]n individual may file with the Commissioner a written complaint against an organization for contravening a provision of Division 1 or for not following a recommendation set out in Schedule 1." Divisions 1 and 2 outline organizations' responsibilities to comply with Schedule 1 and the Privacy Commissioner's powers of oversight and investigation. Section 5 states:

(1) Subject to sections 6 to 9, every organization shall comply with the obligations set out in Schedule 1.

Meaning of "should"

(2) The word "should", when used in Schedule 1, indicates a recommendation and does not impose an obligation.

Appropriate purposes

(3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

*Id.* §5.

<sup>292</sup> *Id.* §§ 1112.

<sup>293</sup> See *Englander v. Telus Communications Inc.*, [2003] F.C.J. No. 975. A precedent "capping" the powers of the Privacy Commissioner came with the recent decision of *Canada (Privacy Commissioner) v. Canada (Attorney General)*, [2003] B.C.J. No. 1344.

<sup>294</sup> *Englander*, F.C.J. No. 975. See also, Privacy Commissioner of Canada, Press Release of March 20, 2002, at [http://www.privcom.gc.ca/media/nr-c/02\\_05\\_b\\_020320\\_e.asp](http://www.privcom.gc.ca/media/nr-c/02_05_b_020320_e.asp) (discussing the Privacy Commissioner's decision pursuant to PIPEDA on Air Canada's Frequent Flyer Program). Both of these cases, however, considered the use of an individual's personal information in the service provider-consumer relationship. Of these decisions, one holds that complaints to the Privacy Commissioner pursuant to PIPEDA are *ultra vires* in labor collective bargaining issues, despite privacy concerns relating to the use of an email. In *L'Ecuyer v. Aeroport de Montreal* [2003] F.C.J. No. 752, the Trial Division of the Federal Court held that the Privacy Commissioner did not have jurisdiction to investigate an employee's complaint about the employer forwarding her email correspondence regarding an alleged harassment charge to her union representatives during a collective bargaining exercise, relying

¶102 Unresolved disputes can be filed before the Federal Court which has jurisdiction to order remedies including ordering the organization to correct its practices, and/or awarding damages, including punitive damages not to exceed Canadian \$20,000.

*B. Provincial Privacy Legislation*

¶103 The province of Quebec has likely been the most progressive Canadian jurisdiction in defining and protecting a privacy right in the private sector. Adopting statutory protections more similar to civil law protections in Europe, Quebec's Charter provides a right to privacy in one's private life.<sup>295</sup> Its Act Respecting the Protection of Personal Information in the Private Sector (1994) applies to all private sector disputes including employer-employee rights. Furthermore, the Civil Code creates a statutory tort regarding the right to privacy.<sup>296</sup>

¶104 With respect to employer-monitoring and PIPEDA, so far only British Columbia and Alberta have adopted legislation that is "substantially similar" to PIPEDA.<sup>297</sup> This legislation was effective January 2004.<sup>298</sup> Ontario has introduced legislation that may pass in 2004 that would also meet the "substantially similar" requirements of PIPEDA.<sup>299</sup> PIPEDA requires the Canadian Privacy Commissioner to report to Parliament annually on "the extent to which the provinces have enacted legislation that is substantially similar" to PIPEDA.<sup>300</sup>

¶105 Table 2 presents a summary of federal and provincial law relevant to electronic employee monitoring in Canada.

Table 2. Summary of Canadian Workplace Privacy Law Relevant to Electronic Monitoring of Private Sector Employees

Source of Law	Summary of Law	Protection for Employees?	Type of Remedy: Civil, Criminal
Charter of Rights and Freedoms	Section 8 protects against unreasonable search and seizure and includes a privacy right.	Public employees. Private employees by analogy only.	Civil damages Criminal penalties
Criminal Code	Section 184 prohibits the interception of private communications by any means.	Yes	Civil Damages Criminal Penalties
PIPEDA	Contains mandatory standards for the collection, use, storage and transmission of personal information	Yes, but only after January 1, 2004 and subject to exemptions regarding	Civil Damages. Criminal where there is proven obstruction of Privacy Commissioner's investigation into an individual complaint, potentially leading to a

on the sole jurisdiction of arbitrators in collective bargaining disputes. *See* Weber v. Ontario Hydro [1995] S.C.R. 929 (Can.).

<sup>295</sup> Quebec Charter of Human Rights and Freedoms (S.Q. 1990, c. 1, s. 5).

<sup>296</sup> The Province of Quebec is the only civil law jurisdiction in Canada. The provinces of British Columbia, Manitoba, Saskatchewan and Newfoundland have also created statutory rights to privacy although only Quebec specifically protects employee privacy. *See respectively*, British Columbia: Privacy Act, R.S.B.C. 1996, c. 373, s. 1(1); Manitoba: Privacy Act, R.S.M. 1987, c.P-125, S. 2(1); Saskatchewan: Privacy Act, R.S.S. 1978, C P-24, as amended R.S.S. 1979, C. 69, s.3; Newfoundland: An Act Respecting the Protection of Personal Privacy, S.N. 1981, C.6, S.3(1). For a general discussion on the relatively inconclusive common law on the existence of a tort of invasion of privacy, see PHILIP H. OSBORNE, THE LAW OF TORTS (2000) (Chapter 4).

<sup>297</sup> As they wait to see if their respective legislation finds federal approval, the Privacy Commissioners of B.C. and Alberta are working to harmonize their legislation, respectively the *Personal Information Protection Act* and the *Personal Information Protection Act*, with PIPEDA. *See* Privacy Commission of Canada, *Federal, British Columbia and Alberta Commissioners Working Together to ensure Seamless Privacy Protection in the Private Sector*, January 26 2004, available at [http://www.privcom.gc.ca/media/nr-c/2004/nr-c\\_040126\\_e.asp](http://www.privcom.gc.ca/media/nr-c/2004/nr-c_040126_e.asp) (last visited Jan. 31, 2004). *See also infra* note 279.

<sup>298</sup> *Id.*

<sup>299</sup> *Id.*

<sup>300</sup> PIPEDA, *supra* note 49 § 25(1). Under PIPEDA, the Governor-in-Council may pass an order on the recommendation of the Minister of Industry, exempting provinces with substantially similar legislation, or organizations subject to such legislation, from the application of PIPEDA. *Id.* § 26.

		substantially similar legislation	summary conviction and fine.
Provincial Privacy Legislation	Privacy legislation similar to the Federal Privacy Act. New legislation in response to PIPEDA that satisfies the "substantially similar" requirement	In British Columbia and Alberta	Civil Damages and/or Criminal – see provincial laws.
Statutory Tort to Privacy	Quebec, British Columbia, Saskatchewan, Manitoba and Newfoundland have relevant statutory torts		

## VI. COMPARATIVE ANALYSIS

¶106 The regulation assessments completed in Sections III, IV and V reveal important inconsistencies in the jurisdictions observed regarding the level of employee privacy in workplace technology systems. Clearly, each region surveyed recognizes to some degree an employee's expectation of privacy in his or her electronic communications made on employer-provided computer systems. The variance is in the level of protection afforded those communications in light of the employer's declared business needs, ranging from system operation and security to monitoring employee workplace misconduct. What emerges is a clear illustration of the value a country or region assigns market needs (i.e., the employer's needs) versus, at the core, fundamental human rights of the individual, here the individual employee. Consistent with its generally pro-market approach to the technology revolution, U.S. regulation offers little protection for employee privacy rights in electronic communications.<sup>301</sup> In contrast, the historic and pervasive value assigned privacy as a fundamental human right in the EU and Canada has resulted in some rather extensive regulation of how employers handle employee personal data gleaned from electronic sources.

¶107 Also apparent from an examination of the jurisdictional variance are non-partisan principles that are fundamental to employee privacy in light of technological advances and the evolution of the modern day workplace. These principles are drawn mostly from EU and Canadian regulation, but are also reflected in U.S. federal law dealing with management of sensitive medical data. They are:

1. Legitimacy. Electronic monitoring should be implemented only where necessary to satisfy the employer's legitimate purpose. Legitimate purposes include those that are necessary for compliance with a legal obligation of the employer, or necessary for the performance of a contract between the employer and the employee, or necessary to ensure system security and proper functioning. If there is a less intrusive means to satisfy the employer's purpose, those means should be implemented.
2. Transparency. The employer's purpose in electronically monitoring employees must be clearly identified and communicated to employees subject to monitoring. All information related to the collection and further processing of data retrieved via electronic monitoring must be disclosed, preferably in a privacy policy. Employees should be informed on how to access this data to ensure its accuracy, how to make corrections and how to complain when they believe their rights have been violated by the employer. Employee consent to the policy may be relevant, but should not be relied on where the consent is not entirely voluntary. Only in very exceptional circumstances will it be acceptable to monitor employee electronic communications covertly.
3. Proportionality. Personal data managed by the employer must be relevant and not excessive in relation to the legitimate purpose for which it is collected and processed. Only in very exceptional circumstances will it be acceptable to monitor the personal content of an

<sup>301</sup> See generally Lessig, *supra* note 51.

electronic communication without violating this principle.

4. Finality. Personal data may only be processed for a specific, explicit and legitimate purpose and not processed in any way incompatible with that purpose. Personal data may be retained only so long as necessary to fulfill the stated purpose.
5. Data Accuracy and Security. Employers are held accountable for maintaining the accuracy of the data and for providing it a secure environment. Data should be accessible only to those personnel with a need to use the data and only after appropriate training in data management and under appropriate supervision.

¶108 The level of government recognition and accommodation afforded these fundamental privacy principles is consistent with the value attributed to market needs versus individual human rights in each of the geographic areas studied. Ultimately, the United States is at the low end of the spectrum for recognizing employee privacy rights. The EU is at the high end, and Canada is somewhere in between. As revealed in the analysis that follows, U.S. regulation of electronic monitoring of employee communications requires simply that employers "rationalize" electronic surveillance. Canada's regulation draws on historic Charter values and now established EU privacy regulation to incorporate a "reasonableness" approach. And the EU prioritizes employee privacy as a fundamental right to require that employers "justify" electronic monitoring in light of the broad protection attributed personal data in that region.

¶109 The U.S. reveres individual liberty, but simultaneously treats rights derived from liberty as personal property. Privacy is a commodity that belongs to each individual to do with as the individual pleases. Thus, the right to privacy held by an employee may be bargained away in exchange for employment. In theory, an employee's liberty should include the liberty to engage in the bargain. Consistent with these premises, U.S. regulation of employer electronic monitoring permits employers to electronically monitor employees so long as the employee has provided consent, including implied consent that arises from an employee's knowledge of an employer's monitoring policy and decision to continue working for that employer. Consent legitimizes employers' interception and/or access to stored electronic communications sent or received by employees. Both federal law under the ECPA and the patchwork of state statutes on the subject recognize consent as the paramount means for sanctioning electronic monitoring of employees. Employers may therefore rationalize the invasion of employee privacy that results from electronic surveillance by proof of employee consent. Express consent given after full disclosure of the employer's intent to intercept or access email or Internet communications is truly the best way to avoid litigation involving privacy matters under existing U.S. law.<sup>302</sup>

¶110 Thus, it is not difficult to "rationalize" electronic employee monitoring in the U.S. Disclosure or "transparency" (in EU terminology) is the preeminent principle for employee privacy under this framework. Under current judicial interpretation of federal and state privacy statutes, a U.S. employer can be confident about implementing an electronic employee monitoring policy so long as it has satisfied the transparency principle and subsequently obtained employee consent. With few exceptions other than those related to employee medical information, there are no limits on the extent of data gathered through electronic monitoring or on the means used to monitor so long as the employer can prove disclosure and consent. Personal communications are subject to surveillance as no proportionality limitation is in place to restrict the employer from accessing communications that are clearly personal in nature.<sup>303</sup> There is no such thing as "covert" monitoring under this construct as the employee ostensibly knows and has agreed to be monitored at the discretion of the employer.

---

<sup>302</sup> See DAVID M. SAFON, WORKPLACE PRIVACY: REAL ANSWERS AND PRACTICAL SOLUTIONS 101 (Thompson Publishing Group) (2000).

<sup>303</sup> Recall that in *Fischer v. Mount Olive*, the court held the employer should have ceased interception of the employee's telephone conversation as soon as it was apparent to the employer that the call was not of a business nature. See notes 222-227, *supra*, and accompanying text. However, in that case, the employer did not have a policy in place disclosing to employees its intent to monitor and as such, the consent exception to the ECPA was inapplicable. See *id.*

¶111 In contrast to the U.S. laissez-faire approach, Canada has adopted a "reasonableness" approach to the issue of employee privacy. In the context of employee electronic monitoring, there must be a balance between the employees' right to privacy and the right of employers to intrude on that right in furtherance of managerial need. Based on existing case law and scholarly opinion, factors that may be instructive to judicial interpretation of that balance will likely include the reasonableness of the grounds and manner of electronic surveillance, and whether there were less invasive alternatives to satisfy the employer's prerogatives, both related to the legitimacy principle identified here.

¶112 With the implementation of PIPEDA, Canadian regulation of employer electronic monitoring may become more specific with respect to what is "reasonable." The standards adapted from the Model Code as Schedule 1 to PIPEDA reflect the influence of the EU Privacy Directive and should mandate employer respect for the five privacy principles outlined above. However, there are two noteworthy distinctions. First, PIPEDA's language seems broad enough to allow wide judicial interpretation with respect to the Model Code's standards. For example, employers may need to identify a purpose for electronic monitoring of employees, but the current standards are silent with respect to when such a purpose is "legitimate." This problem may be alleviated by guidelines offered by Canadian privacy authorities similar to those promulgated in the EU such as the U.K. Model Code, or may rest until addressed in the normal course of the common law tradition. Second and more importantly, under PIPEDA "consent" is a factor in determining the reasonableness of personal data collection and dissemination. It remains to be seen whether employee consent to electronic monitoring will provide the broad sanction for employer surveillance as it has under U.S. federal law.

¶113 The regulation in the EU of employee electronic monitoring—albeit derivative of broader data protection legislation under the EU Privacy Directive and national implementing legislation—is the most extensive of the jurisdictions studied. Certainly any employer operating in the EU must have a privacy policy which adequately discloses to employees the reasons for electronic monitoring; the means that will be used to accomplish that monitoring; how long data will be stored and to whom it may be transmitted; how to access data held by the employer and make requests to change inaccuracies; how to object to the monitoring; and finally where and how to seek legal recourse for alleged violations of the employee's rights under the policy. Such disclosure satisfies the transparency principle inherent in EU privacy protection. In fact, an increasing number of employers are adopting "privacy policies" setting out the security measures to be taken and the use that employees may make of the new computer tools made available to them.<sup>304</sup> Some foreign authorities, however, question the legal status of such privacy policies in light of existing privacy law.<sup>305</sup> The prevailing EU opinion is that these policies are rarely negotiated with the employee or his or her proper representative, and reveal a "patent imbalance between the prerogatives of the employer and the rights of employees."<sup>306</sup> Employee consent will not justify monitoring unless the employee has real choice and will not experience a negative job determination for his or her refusal to provide such consent to his or her employer.

¶114 Beyond transparency, employers in the EU must also satisfy the legitimacy principle. That means that the employer must have a legitimate reason to justify electronic surveillance of its employees. Additionally, if there are any less intrusive means available to the employer for satisfying its otherwise legitimate business needs in monitoring, the employer must use those less intrusive means. Only in exceptional circumstances, such as when the employee is suspected of committing a seriously wrongful or criminal act, will it be justifiable to electronically monitor an individual employee. Generally the content of employee electronic communications may not be read or disclosed unless one of these conditions is satisfied, even when the employer has prohibited personal computer use. Moreover, under the proportionality principle in which monitoring is justified, the

---

<sup>304</sup> CNIL Report, *supra* note 62, at 5.

<sup>305</sup> *Id.* at 6.

<sup>306</sup> *Id.* at 5.

employer may only collect data as necessary to alleviate the perceived risk and, under the finality principle, may only use the data collected for that purpose. Finally, the employer must be prepared to provide the best security for any employee personal data that is processed in connection with electronic monitoring. This can be a costly proposition considering the requirements for appropriate software and necessary management training.

¶115

Table 3 presents a summary of the practical application of the fundamental privacy principles derived from this comparative analysis. The table reveals the variation in substance and practical application of data privacy requirements amongst the EU, the United States and Canada. The left column highlights the privacy principles implicated in the following categories: reasons supporting electronic monitoring of employees, acceptable methods of electronic employee monitoring, the substance of what may be monitored, and relevant data management requirements. The table then summarizes for each of the EU, the United States and Canada the regulatory requirements for each identified category to the extent that requirements exist.

Table 3. Summary Comparison of the Regulation of Employee Electronic Monitoring in the EU, United States and Canada

	EU	U.S.	Canada
Reasons Supporting Employer Monitoring of Employee Electronic Communications  Privacy Principles Implicated: Legitimacy Transparency Finality	Monitoring must be necessary to complete a contract with the employee, or to comply with a legal obligation of the employer, or necessary for the legitimate business interests of the employer so long as the employee's fundamental rights are not violated.	Reasons for monitoring are important under the NLRA, the ADA, and under the ECPA. The ECPA's exception that permits monitoring involving interception of the contents of electronic communications while in transit is only available to a provider of a computer system and only permits monitoring in the ordinary course of business. Providers do not need a reason to monitor the contents of stored electronic communications or to monitor with employee consent. The employer's policy may constitute implied consent. The ADA requires that inquiries about employees' medical information be job related; employee consent is not a defense to unlawful inquiries. The employer's reasons for monitoring are relevant under the NLRA to assess whether surveillance is unlawful.	Reasons for employee surveillance must be grounded in "reasonableness" and must be identified, disclosed and consented to under PIPEDA.
Acceptable Methods of Electronic Monitoring of Employees  Privacy Principles Implicated: Legitimacy	Type of monitoring must be tailored to the perceived risk to the employer. No continuous automatic monitoring of individual workstations. Method may monitor network traffic data, size and type of attachments to	Type of monitoring is restricted by the ECPA when it involves interceptions or access to the contents of electronic communications., unless the employee or other party has given consent, or the employer is the provider of the system.	Methods must be "reasonable" and must take into account the availability to the employer of other alternatives. Interception is permissible where

Transparency Proportionality	communications. No covert tactics, including interception of data in transmission, unless exceptional circumstances exception applies.	The employer's policy may constitute implied consent. Some state laws restrict covert monitoring unless exceptional circumstances apply. Additionally, the NLRA may require transparency by requiring the employer to bargain monitoring policy in advance of imposing it.	employee consent is provided. Assuming compliance with PIPEDA's Model Code standards, employers may collect personal information using "fair and lawful means."
Substance of What May be Monitored  Privacy Principles Implicated: Legitimacy Transparency Proportionality Finality Accuracy/Security	May monitor network traffic data and size and type of attachments to ensure system security. May not monitor communication for content unless exceptional circumstances exception applies. Even under those circumstances, some Member States prohibit content monitoring outright where communication is clearly personal in nature.	May monitor network traffic data and size and type of attachments without violating the ECPA or ADA. Content monitoring is regulated by the ECPA, unless an exception applies consent or one of the other exceptions under the ECPA applies. Additionally, the ADA prohibits disability-related inquiries unless job related. NLRA prohibits surveillance that targets protected, concerted activities of employees.	No explicit restrictions. However, employers may only collect personal data relevant to their reasonable managerial purposes for engaging in monitoring conduct.
Data Management Requirements Privacy Principles Implicated: Transparency Finality Accuracy/Security	Data may only be retained so long as necessary to satisfy the employer's justification and may not be processed in any way inconsistent with that purpose. In no cases may data be held longer than 3 months. Data security must be maintained at all levels and at all cost.	Consent is required before employer may divulge the contents of covered electronic communications to others. ADA and HIPAA (for self-insured employers) restrict disclosure of medical and health information. ADA restricts processing of medical information except for limited job related reasons. Data security safeguards are required under both the ADA and HIPAA.	Security safeguards must be implemented to protect employee personal data that is collected. The data collected must be accurate and complete and may only be retained so long as necessary to fulfill employer's purpose.

## VII. CONCLUSION

¶116

The task of supervising employees has no doubt been radically changed by the use of electronic communications technology in the workplace. The productivity of employees may be enhanced by the same technology that provides new ways that enable employees to waste time on the job, harass other employees, or improperly disclose trade secrets and confidential information. Advances in technology related to electronic monitoring enable employers to take advantage of new opportunities to achieve enhanced workplace productivity and to counter new opportunities for employees to engage in misconduct. There are clearly valid business reasons for employers to use some forms of electronic monitoring. It is unlikely that any country will enact laws that prohibit all electronic workplace monitoring, even one with a strong culture of workplace privacy. Instead, electronic workplace monitoring laws are enacted in a context that generally recognizes the valid business reasons for electronic monitoring and considers the interests of employees in workplace privacy. In

this respect the EU, United States, and Canadian approaches are similar; all give some due to the business reasons for electronic monitoring.

¶117 Indeed, the privacy of employees may be profoundly impacted by electronic monitoring practices in the workplace. Most employees use some form of electronic communication technology on the job, whether it be email access, Internet access, or other computer technology. Many employees are permitted to make some personal use of the electronic communications technology on the job. Where employers have not expressly granted this permission to employees, pragmatic employers may at least anticipate that personal use will be made by employees from time to time. However, when employers then use electronic monitoring to access employees' personal email or Internet communications, employers gain access to personal information about employees. Such electronic monitoring practices bring the very real privacy interests of employees into clear conflict with employers' business interests. The possibility of secret electronic monitoring by employers only exacerbates that conflict.

¶118 It is in this context that the EU, Canada, and the United States take radically different approaches to regulating electronic monitoring. The EU starts with the premise that employees have fundamental privacy interests in personal information, broadly defining personal information to include email and other electronic communications containing employees' personal information, even when doing so may limit employers' ability to read the contents of employees' personal email made on employers' computer systems. Canada takes a more balanced approach, recognizing that employees have important privacy interests in their personal information, but requiring a balancing of the employees' privacy interests with the rights of employers to intrude in order to protect legitimate business interests. When the workplace privacy laws of the EU, Canada, and the United States are compared, the privacy laws of the EU and Canada seem more alike than different. In contrast, the laws of the United States stand out as providing little protection for employees' personal information or employees' personal communications made in the workplace. Indeed the United States generally fails to protect the privacy of employees' personal information except in limited circumstances that generally relate to medical and health information, or when the contents of personal communications are intercepted or accessed by means that are specifically prohibited by statute and not immunized by one of many seemingly management-friendly exceptions.

¶119 At the present, a comparison of workplace privacy laws in the EU (and its Member States), Canada, and the United States fails to reveal a common legal paradigm for multinational employers that would support a uniform electronic monitoring policy for all employees working in these countries. The lack of a common legal paradigm for the EU, Canada, and the United States is due to inconsistencies in the privacy laws and underlying value systems of the different countries, and the variety of factors that alter the lawfulness of employee electronic monitoring from country to country. There is hope that a paradigm will emerge as workplace specific law and regulatory guidance on the lawfulness of electronic workplace monitoring practices continues to evolve in all of these countries, and that the paradigm will be grounded in equitable principles such as those that emerge from the comparative analysis in Section VI above.

¶120 In the EU, some Member States, such as the U.K., have issued non-binding guidance on electronic workplace monitoring practices, and other industry and government organizations are tackling the issue. However, much more legislation and guidance is needed before a common legal paradigm for electronic monitoring practices within the Member States of the EU will emerge. Although Canada has enacted legislation that resembles the privacy protections for personal information found in the EU Privacy Directive, Canada also lacks specific legislation or guidance on electronic workplace monitoring practices. Likewise in the United States, a multitude of privacy laws could be used to define the parameters of electronic workplace monitoring and the privacy rights of employees. Yet few of these laws have been applied in ways that restrict electronic monitoring practices. Where United States laws have been applied, the sanctions for violating the laws appear to provide harsher penalties for employers than penalties for privacy violations found under EU or Canadian laws. Thus, there are few "legal" incentives for employers in the United States to

voluntarily promise privacy rights for employees that would equal the privacy protections for employees found in the EU or Canada. Under existing U.S. laws, a U.S. employer that makes such promises may incur expensive legal liability if it later breaches those promises, even if the breach is for unanticipated reasons like preventing or detecting employee misconduct. The increased risk of liability for U.S. employers may be at least partially offset by carefully crafted privacy policies that include disclaimers and exclusions for unanticipated circumstances.

¶121 No law in the United States, Canada, or the EU will prevent an employer from embracing the fundamental privacy principles of legitimacy, transparency, proportionality, finality and data accuracy and security. In fact, much insight into the privacy issues related to electronic workplace monitoring will be gained by employers who understand and apply these principles. When employers can realistically assess the privacy implications of proposed electronic monitoring practices, they may *in fairness* choose to tailor their electronic monitoring practices to balance employees' privacy interests with legitimate business concerns. They may choose to honor employee privacy rights in a way that is not yet universally required by the rule of law. Such a result would be a true reward of this comparative law study.