University of Florida Journal of Law & Public Policy

Volume 19 | Issue 3 Article 2

2008

Workplace Electronic Privacy Protections Abroad: The Whole Wide World is Watching

William A. Herbert

University of Florida
Journal of Law and Public Policy

VOLUME 19 DECEMBER 2008 NUMBER 3

ARTICLES

WORKPLACE ELECTRONIC PRIVACY PROTECTIONS ABROAD: THE WHOLE WIDE WORLD IS WATCHING

*William A. Herbert**

I. INTRODUCTION 380

II. AN OVERVIEW OF FUNDAMENTAL EUROPEAN PRIVACY PROVISIONS 385
A. *Convention for the Protection of Human Rights and Fundamental Rights* 385
B. *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data* 387
C. *The 1995 European Privacy Directive* 388
1. Substantive Scope of the Privacy Directive 388
2. The Establishment of Supervisory Authorities in Member States 390
3. The Article 29 Working Party 391
4. Safe Harbor Framework for Transfer of Personal Data to and From the United States 391

* Mr. Herbert is Deputy Chair and Counsel for the New York State Public Employment Relations Board (PERB). The opinions expressed in this Article are Mr. Herbert's personal views and do not reflect the views of PERB or the State of New York. An earlier draft of this Article was presented at the 61st Annual Conference on Labor at New York University School of Law. This Article is dedicated to PERB Chairman Jerome Lefkowitz who, through his intellectual vigor, pragmatism, and humility, has inspired a generation of public sector labor attorneys, arbitrators, and mediators. Mr. Herbert would like to express his appreciation to Professors L. Camille Hebert, Ann C. Hodges, Samuel Estreicher, and Miriam A. Cherry, who each, in their own way, assisted in the development of this Article. Finally, Mr. Herbert must thank Judith A. Lee for her patience, wisdom, and fortitude over the past three decades.

5. 2002 Directive on Privacy and Electronic Communications 393
6. European Commission Staff Working Document: Early Challenges Regarding the "Internet of Things" 394
D. *The Charter of Fundamental Rights* 395

III. RELEVANT DECISIONS BY THE EUROPEAN COURT OF HUMAN RIGHTS 396

IV. ARTICLE 29 WORKING PARTY OPINIONS AND WORKING DOCUMENTS 403
A. *Opinion on the Processing of Personal Data in Employment* 403
B. *Working Document on Surveillance of Workplace Electronic Communications* 405
C. *Working Document on Biometrics* 407
D. *Opinion on the Use of Employee Location Data* 408

V. UNITED KINGDOM 409

VI. FRANCE 414

VII. CANADA 416

VII. CONCLUSION 419

I. INTRODUCTION

Novelist Jonathan Franzen has aptly described the right to privacy in the United States as being "the Cheshire cat of values: not much substance, but a very winning smile."[1] In fact, an enforceable right to privacy, in the contemporary American electronic workplace, has not yet materialized, with or without a smile.

Despite the enormous technological transformation of the workplace over the past three decades,[2] the scope of workplace privacy protections in the United States remains quite limited. This porosity of privacy in American labor and employment law stems from the narrow scope of the

1. Jonathan Franzen, *Imperial Bedroom*, *in* How To Be Alone: Essays, 39, 42 (2002).
2. *See* U.S. DEP'T OF LABOR, REPORT ON THE AMERICAN WORKFORCE 5 (2001).

six primary sources of rights relevant to workplace privacy: (a) the Fourth Amendment to the U.S. Constitution,[3] which has been interpreted to grant public sector employees a limited right to privacy;[4] (b) federal statutes containing privacy restrictions applicable to employment;[5] (c) state constitutional right to privacy clauses;[6] (d) state privacy legislation;[7] (e) state common law;[8] and (f) negotiated provisions contained in collective bargaining agreements.

In contrast to the common misperception, the U.S. Constitution "does not explicitly mention any right of privacy."[9] Constitutionally based privacy rights in the United States have been the result of judicial interpretations of constitutional amendments that were ratified in 1789 and 1869.[10] Many of those interpretations are subject to sustained criticisms

---

3. The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

4. *See* O'Connor v. Ortega, 480 U.S. 709, 714-17 (1987).

5. *See, e.g.*, Privacy Act of 1974, 5 U.S.C. § 552a (2008); Americans with Disabilities Act, 42 U.S.C. §§ 12101-12213, 12112(d) (2008); Electronic Privacy Communications Act, 18 U.S.C. § 2510; 18 U.S.C. § 2701; Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d-2 (2008).

6. *See* CAL. CONST. art. I, § 1; ILL. CONST. art. I, § 6; HAW. CONST. art. I, § 6. Unlike other states, California's constitutional right to privacy provision prohibits privacy intrusions by both governmental and private actors. *See* Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 644 (Cal. 1994).

7. An example of a relatively recent state privacy statute is the New York Labor Law section 203-c, which prohibits both private and public employers from videotaping employees in restrooms, locker rooms, or other rooms designated for undressing. *See* N.Y. LAB. LAW § 203-c (McKinney 2008). Other states have enacted statutes restricting, to a limited degree, employer computer surveillance. *See infra* note 21 and accompanying text.

8. *See generally* RESTATEMENT (SECOND) OF TORTS §§ 652A-E (1997) (defining four privacy torts: unreasonable intrusion upon seclusion; appropriation of the name or likeness of another; unreasonable publicity given to private life; and publicity that unreasonably places another in a false light). The common law in some states recognizes one or more of these privacy torts.

9. Roe v. Wade, 410 U.S. 113, 152 (1973).

10. *See* Mapp v. Ohio, 367 U.S. 643, 646-58 (1961); Griswold v. Connecticut, 381 U.S. 479, 484-86 (1965); Lawrence v. Texas, 539 U.S. 558, 578-79 (2003).

and continue to be regular subjects of questioning during Supreme Court judicial confirmation hearings.[11]

The American legal framework is narrow in stark contrast to the public perception that privacy constitutes an enforceable and unbridled American right. This misperception is greatest within the workplace, where employees frequently assume that there are strict legal restrictions on employer surveillance.

The American habit of relying on litigation, rather than legislation and regulation, as a primary means for the development of a public policy framework in certain areas ensures that American privacy law will not keep pace with rapid technological advances occurring in the workplace. Litigation provides only post-hoc resolution of complicated issues at the crossroads of technology and labor law. Moreover, as two scholars have noted "[t]he reactive, adaptive process adopted by the courts makes it difficult to address digital privacy problems rationally or effectively."[12]

At the same time, legislative action is too frequently precipitated by tragedy or other notorious events at the expense of sober, proactive, and rational inquiry into a developing problem. A good example of such legislative over-exuberance is the Videotape Privacy Protection Act,[13] which stemmed from the noxious release of video rental records of Supreme Court nominee Robert Bork.[14] While video rental privacy is deserving of legislative attention, broader electronic workplace privacy issues have received very little legislative attention in the past two decades. The recent enactment of the Genetic Information Nondiscrimination Act of 2008 (GINA)[15] is a prime exception to the general lack of legislative initiative in the area of workplace privacy issues.

One commentator has asserted that the current American privacy law paradigm is reflective of a contemporary cultural preference for digital conveniences over expectations of privacy.[16] According to this commentator, consumer and public embracement of new technologies may mean the end to any privacy expectations. In a rapid response, Professor Daniel J. Solove challenged those assertions, noting that an inherent caveat

---

11. *See generally* ROBERT H. BORK, THE TEMPTING OF AMERICA 110-15 (1990); STEPHEN L. CARTER, THE CONFIRMATION MESS 54-61 (1994).

12. Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground,* 2 U. OTTAWA L. & TECH. J. 357, 361-62 (2005).

13. 18 U.S.C. § 2710 (2008).

14. Consumer Privacy Guide.org, Video Privacy Protection Act of 1988, http://www.consumerprivacyguide.org/law/vppa.shtml (last visited Nov. 19, 2008).

15. Genetic Information Nondiscrimination Act, Pub. L. No. 110-233, 122 Stat. 881 (2008).

16. L. Gordon Crovitz, *Privacy? We Got Over It,* WALL ST. J., Aug. 25, 2008, at A11.

underlying an individual providing electronic data to institutions, such as banks, is that the institutions will treat the information confidentially.[17] This exchange is emblematic of an accelerating distance between American law and societal expectations stemming from digital innovation.

While computer scientists work toward a construct enabling the amalgamation of information from multiple technological sources to create individual digital data trails,[18] there is little parallel work being done to develop legal protocols and guidelines aimed at regulating the use of such collective intelligence. Although analyses of merged digital information about behavior in the workplace can lead to positive results, including improved efficiencies, there remains a need for joint legal and technological research projects aimed at developing prudent limitations on the use of such accumulated collective intelligence. Without regulatory and architectural checks, collective intelligence can be easily misused to restrict and restrain individual and collective rights and expectations in the workplace.

The limits of American electronic privacy protections were highlighted almost a decade ago, when a European governmental entity concluded that the "current [American] patchwork of narrowly-focused sectoral laws and voluntary self-regulation cannot at present be relied upon to provide adequate protection in all cases for personal data transferred from the European Union."[19] Although subsequent negotiations between the United States and the European Union have established a safe harbor for American companies to overcome the limitations of American privacy law,[20] the codification of electronic workplace privacy laws in the United States has not materialized on the national or state level.[21]

For the past three decades, deregulation ideology has dominated most public policy discussions in the United States, especially in the area of

---

17. *See* Daniel J. Solove, *Fallacies About Privacy*, CONCURRING OPINIONS, Aug. 25, 2008, http://www.concurringopinions.com/archives/2008/08/fallacies_about.html#more.

18. John Markoff, *You're Leaving a Digital Trail, Should You Care?*, N.Y. TIMES, Nov. 30, 2008, *available at* http://www.nytimes.com/2008/11/30/business/30privacy.html.

19. Opinion 1/99 of the Working Party Concerning the Level of Data Protection in the United States and the Ongoing Discussions Between the European Commission and the U.S. Government, at 2 WP (1999) 15 final (Jan. 26, 1999), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp15en.pdf (last visited Nov. 19, 2008).

20. *See infra* note 71 and accompanying text.

21. At least two states, Delaware and Connecticut, have enacted laws requiring particular employer notification to employees before conducting electronic monitoring. *See* DEL. CODE ANN. tit. 19, § 705 (2008); CONN. GEN. STAT. § 31-48d (2008).

labor and employment law.[22] This ideology, along with the decline in union density, inherently delegates to employer self-regulation the task of determining the proper balance between employer and employee interests. While it is not uncommon for employers to respect employee privacy to some degree for numerous business reasons, such voluntary employer balancing results in few, if any, enforceable workplace rights.

In *Guard Publishing Company d/b/a The Register-Guard*,[23] the National Labor Relations Board concluded that an employer's common law personal property rights, with respect to its computer system, trumps the statutory associational rights granted by the National Labor Relations Act.[24] The decision is one indication of the current American legal landscape with respect to employee legal rights in an electronic workplace.

The severity of the current worldwide economic crisis, however, may result in a public policy shift in favor of workplace privacy regulations. In response to the consequences of the current recession, French President Nicolas Sarkozy has stated: "Le laisser-faire, c'est fini."[25]

In contrast to the United States, the European Union and its Member States, along with other industrialized countries such as Canada, have been proactive in developing a substantive and procedural legal structure for protecting individual and personal data privacy.[26] This proactive effort stems from an alternative perspective that approaches privacy as constituting a component of human dignity, rather than as an extension of property rights.[27]

Within Europe, the scope and applicability of privacy rights emanate from certain primary sources:[28] the codification and regulation of individual and data privacy under the Convention for the Protection of Human Rights and Fundamental Freedoms; the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data; the European Privacy Directive and national legislation; the

---

22. *See* William A. Herbert, *The Electronic Workplace: To Live Outside the Law You Must be Honest*, 12 EMP. RTS. & POL'Y J. 49, 55 (2008).

23. 351 N.L.R.B. No. 70 (2007).

24. *See id.* at 9-10.

25. Roger C. Altman, *The Great Crash, 2008*, 88 FOREIGN AFF. 2-14 (2009), *available at* http://www.foreignaffairs.org/2009/1.html.

26. *See* Export.gov, Welcome to the Safe Harbor, http://www.export.gov/safeharbor (last visited Nov. 17, 2008).

27. *See* Gail Lasprogata et al., *Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada*, 2004 STAN. TECH. L. REV. 4, 8-9 (2005).

28. *See id.* at 9-14, 37-40.

establishment of governmental agencies in each country with the power to enforce privacy statutes and regulations; and the creation of an international body, known as the Article 29 Working Party, to provide analysis and guidance with respect to privacy issues.

This Article examines how the European Union, the United Kingdom, France, and Canada have approached workplace privacy issues in response to the advent of new workplace technologies. Where appropriate, this Article will compare the approach abroad to the current state of American labor and employment law. The presentation of alternative approaches, however, should not be perceived as suggesting that one or more of these approaches constitute some sort of legal panacea. Rather, the analyses and proactive choices made by other jurisdictions provide alternatives worthy of consideration in examining the proper balance of rights and interests in the American electronic workplace.

This Article begins with an examination of the European sources of law that establish individual and personal data privacy as fundamental rights. It then turns to a discussion of relevant precedent from the European Court of Human Rights, followed by an analysis of various important opinions and working documents from the Article 29 Working Party. The Article then examines the applicable law in the United Kingdom, France, and Canada. Finally, the Article calls for a reevaluation of American public policy through examination of the principles, guidelines, and structures adopted in other industrialized countries.

II. AN OVERVIEW OF FUNDAMENTAL EUROPEAN PRIVACY PROVISIONS

A. *Convention for the Protection of Human Rights and Fundamental Rights*

In April 1950, the Council of Europe adopted the Convention for the Protection of Human Rights and Fundamental Rights, commonly referred to as ECHR.[29] Since its adoption, ECHR has been amended multiple times

29. The Council of Europe is distinct and a much older European institution than the European Union. The Council of Europe is an intergovernmental entity formed in 1949 with a current membership of 47 countries. For comparison, see Council of Europe and European Union, http://www.coe.int/t/dg3/romatravellers/Documentation/LOEEU_en.asp (last visited Nov. 17, 2008). In contrast, the European Union has 27 Member States. The European Union has established various international bodies including the European Parliament, the European Commission, and the Council of the European Union. *Id.*

and ratified by Member States.[30] ECHR grants broad privacy protections in both the public and private sectors.

ECHR, Article 8, section 1 establishes privacy as a fundamental right: "Everyone has the right to respect for his private and family life, his home and his correspondence."[31] In certain circumstances, however, pursuant to ECHR, Article 8, section 2, public entities are permitted to interfere with an individual's rights, if it is in accordance with domestic law and such interference is "necessary in a democratic society."[32] ECHR, Article 8, section 2 states:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[33]

Pursuant to Article 6, section 2 of the Treaty of the European Union, the European Union and its Member States are required to respect the fundamental rights granted by ECHR.[34]

Finally, ECHR establishes an international tribunal for the resolution of alleged violations of such rights by Member States: the European Court of Human Rights.[35] The European Court of Human Rights has issued a number of significant decisions that have applied ECHR, Article 8, to employer monitoring.[36]

---

30. *See* Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221, http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/EnglishAnglais.pdf (last visited Nov. 17, 2008) [hereinafter ECHR].

31. *Id.* art. 8, § 1.

32. *Id.* art. 8, § 2.

33. *Id.*

34. *See* Treaty of Amsterdam Amending the Treaty of the European Union and of the Treaty Establishing the European Communities and Certain Communities and Certain Related Acts, Oct. 2, 1997, 1997 O.J. (C340), *available at* http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:321E:0001:0331:EN:PDF.

35. *See* ECHR, *supra* note 30, arts. 19-51.

36. *See* Halford v. United Kingdom, 24 Eur. Ct. H.R. 523 (1997); Copland v. United Kingdom, 45 Eur. Ct. H.R. 253 (2007).

B. *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data*

In January 1981, the Council of Europe adopted the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data[37] (Personal Data Convention) aimed at protecting a right to privacy with respect to the automatic processing of personal data. Chapter II, Article 5, of the Personal Data Convention requires signatory countries to modify their respective national laws consistent with the basic principles of the Personal Data Convention.[38] These basic principles require that the personal data be:

1. obtained and processed fairly and lawfully;[39]
2. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;[40]
3. adequate, relevant and not excessive in relation to the purposes for which they are stored;[41]
4. accurate and, where necessary, kept up to date;[42]
5. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored;[43]
6. protected through appropriate security measures to avoid accidental or authorized destruction, access, alteration or distribution;[44]
7. accessible to the subject of the data to establish the existence and general content of the automated personal data file;[45] and
8. subject to rectification or erasure if the data was processed contrary to the provisions of the national law enacted to

37. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, ETS No. 108, http://conventions.coe.int/Treaty/en/Treaties/Html/08.htm (last visited Nov. 17, 2008) [hereinafter Personal Data Convention].

38. *See id.* ch. II, art. 4.

39. *Id.* ch. II, art. 5.

40. *Id.*

41. *Id.*

42. Personal Data Convention, *supra* note 37, art. 5.

43. *Id.*

44. *Id.* art. 7.

45. *Id.* art. 8.

give effect to the basic principles of the Personal Data Convention.[46]

In addition, the Personal Data Convention contains restrictions on the gathering of personal data that reveals racial origin, political opinions, religious and other beliefs, as well as personal data concerning health or sexual life and criminal convictions.[47] Automatic data collection with respect to these topics is prohibited unless a subject country has enacted a domestic law that provides sufficient safeguards.[48]

C. *The 1995 European Privacy Directive*

In 1995, the European Parliament and the Council of the European Union issued Directive 95/46/EC (Privacy Directive).[49] A central purpose of the Privacy Directive is to ensure that Member States protect an individual's "right to privacy with respect to the processing of personal data."[50] An equally important objective of the Privacy Directive is to promote legal uniformity among Member States with respect to personal data to ensure a free flow of such data.[51]

1. Substantive Scope of the Privacy Directive

The broad scope of the information protected under the Privacy Directive is demonstrated by the definition of the phrase "personal data": "any information relating to an identified or identifiable natural person ('data subject'); 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."[52]

The Privacy Directive imposes numerous obligations on Member States, including the requirement that each country enact or modify national legislation consistent with the Privacy Directive's uniform

---

46. *Id.*

47. *See* Personal Data Convention, *supra* note 37, art. 6.

48. *See id.*

49. Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L281) 31 [hereinafter Privacy Directive]. An unofficial version of the Privacy Directive is available at http://www.cdt.org/privacy/eudirective/EU_Directive_.html (last visited Nov. 11, 2008).

50. *Id.* art. 1, § 1.

51. *Id.* art. 1.

52. *Id.* art. 2(a).

principles and criteria.[53] When a Member State enacts or modifies national legislation, the Privacy Directive mandates specific criteria to be followed by that Member State. Compliance with the criteria is necessary to ensure that data processing will be deemed legitimate.[54] The criteria require that:

A. the data subject has unambiguously given his or her consent; or
B. [the] processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract; or
C. [the] processing is necessary for compliance with a legal obligation to which the controller is subject; or
D. the processing is necessary in order to protect the vital interests of the data subject; or
E. [the] processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
F. [the] processing is necessary for the purposes of the legitimate interests pursued by the controller or by third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights of the data subject . . .[55]

Every individual subject to personal data collection is guaranteed, under the Privacy Directive, the right to receive confirmation whether his or her personal information is being processed; the purposes of the processing; the categories of the information concerned; and the recipients to whom the information is to be disclosed.[56] In addition, a data subject is entitled to receive in an "intelligible form" the information being processed, along with the rationale underlying any automatic processing.[57] Furthermore, an individual who is the subject of data collection is entitled to object to the processing in particular circumstances.[58]

53. *Id.* arts. 5, 6 & 7.
54. *See* Privacy Directive, *supra* note 49, art. 7.
55. *Id.* art. 7(a)-(f).
56. *See id.* art. 12.
57. *See id.*
58. *See id.* art. 14.

In general, the processing of personal information that can reveal the race, ethnicity, religion, political opinions, philosophical beliefs, union membership, health, and sex life is prohibited.[59] This general prohibition is subject to a number of exceptions, including two that are readily applicable to the workplace: when explicit individual consent has been provided by the employee subject to the data collection; and when the data processing is necessary to carry out the employer's legal obligations, so long as it is authorized by national legislation and includes adequate safeguards.[60]

2. The Establishment of Supervisory Authorities in Member States

In addition to its substantive mandates, the Privacy Directive, Article 28, requires each Member State to establish an independent governmental entity, known as a supervisory authority, to ensure compliance with the national legislation enacted consistent with the Privacy Directive.[61] These supervisory authorities have procedural similarities to many federal and state administrative agencies in the United States. Article 28 of the Privacy Directive mandates that each supervisory authority be granted the following administrative responsibilities and duties:

A. To hear and resolve claims alleging a violation of the rights and freedoms with respect to the processing of personal information;
B. Investigative powers including the power to access the data at issue and to collect information necessary to engage in supervisory duties;
C. To issue opinions with respect to the handling of data as well as the power to order the blocking, erasure or destruction of data; and
D. To commence legal proceedings seeking to enforce national provisions adopted pursuant to the Privacy Directive;
E. To prepare regular reports regarding their activities.[62]

The establishment of national bodies under Article 28 is an important component of the European Union's proactive approach to privacy issues.

---

59. *See* Privacy Directive, *supra* note 49, art. 8, § 1.
60. *See id.* art. 8, § 2(a) & (b).
61. *See id.* art. 28.
62. *See id.*

Each country's supervising authority issues opinions and guidelines that can assist organizations and individuals in complying with the applicable privacy legislation.[63]

3. The Article 29 Working Party

In addition to mandating the creation of an independent national administrative body in each Member State, the Privacy Directive also creates an independent advisory body known as the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data (Article 29 Working Party).[64] The Article 29 Working Party is composed of representatives from the supervising authority of each European Union Member State.[65]

The responsibilities of the Article 29 Working Party are set forth in the Privacy Directive.[66] They include examining national data privacy legislation in Member States to ensure uniformity; examining the national data privacy laws of third-party countries, such as the United States; and issuing opinions and recommendations on issues related to personal electronic privacy.[67] Since its creation, the Article 29 Working Party has issued a number of significant advisory opinions relevant to the workplace which will be discussed in Part IV, *infra*.[68]

4. Safe Harbor Framework for Transfer of Personal Data to and From the United States

Article 25 of the Privacy Directive permits the transfer of personal information to a third country, outside the European Union, only if the third country ensures an adequate level of data privacy protection.[69] When it is determined that a third country,[70] lacks adequate legal protections, the Privacy Directive directs that negotiations take place to remedy those inadequacies.

---

63. *See id.*

64. Privacy Directive, *supra* note 49, art. 29. The website for the Article 29 Working Party is http://ec.europa.eu/justice_ home/fsj/privacy/workinggroup/index_en.htm (last visited Nov. 18, 2008).

65. *See id.*

66. *Id.* art. 30(1).

67. *Id.*

68. *See, e.g.*, *supra* note 19 and accompanying text; *see infra* notes 148, 154, 195 and accompanying text.

69. Privacy Directive, *supra* note 49, art. 25.

70. *See id.*

In 2000, the European Union and U.S. Commerce Department reached an agreement for a "safe harbor" framework aimed at permitting data transfers from European Union Member States to the United States.[71] As part of the agreement, the U.S. Commerce Department issued seven voluntary safe harbor privacy principles applicable to the handling of personal data to qualify for safe harbor status: notice, choice, onward transfer, security, data integrity, access, and enforcement.[72]

These voluntary principles aim to establish an adequate privacy framework to permit American companies to receive personal data originating from an European Union Member State.[73] However, the principles are not applicable to information gathered and processed initially within the United States.[74]

The safe harbor notice principle mandates that an organization provide an individual with initial notice that includes: the purpose for the data collection and how the information will be used; the applicable complaint procedure; the types of third parties to which the information may be disclosed; and the choices and means offered for limiting the use and disclosure of the information.[75]

With respect to consent, an organization under the privacy principles must grant individuals the opportunity to opt out of having personal data disclosed to a third party or used for a purpose inconsistent with the initial notice.[76] However, for data related to medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, or union membership, explicit consent must be obtained before the information is disclosed to a third party or used for an unauthorized purpose.[77]

In addition, individuals must be allowed access to their personal data and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense for such access would be disproportionate to the risks to the individual's privacy or where the rights of persons other than the individual would be violated.[78]

---

71. *See* Export.gov, Safe Harbor Documents, http://www.export.gov/safeharbor/SH_Documents.asp (last visited Nov. 18, 2008).

72. *See* U.S. Dep't of Commerce, Safe Harbor Privacy Principles, July 21, 2000, http://www.export.gov/safeharbor/SH_Privacy.asp [hereinafter Privacy Principles].

73. *See id.*

74. *See id.*

75. *See id.*

76. *See id.*

77. *See* Privacy Principles, *supra* note 72.

78. *See id.*

Under the safe harbor principles, there must be an adequate mechanism created to assure compliance with the principles including a complaint procedure and consequences when the principles are not followed.[79] At a minimum, such mechanisms must include: (a) an available, affordable, and independent process to hear and resolve individual complaints and disputes; (b) follow up procedures for verifying that the assertions about a privacy practice are true and that the privacy practice has been implemented as presented; and (c) an ability to remedy problems arising out of a failure to comply with the principles by organizations announcing their adherence to them and consequences for such organizations.[80]

5. 2002 Directive on Privacy and Electronic Communications

In July 2002, the European Parliament and the Council of the European Union supplemented the Privacy Directive with Directive 2002/58/EC (Directive on Privacy and Electronic Communications),[81] which applies the criteria of the Privacy Directive to personal data transmitted through a publicly available electronic communications service.[82] The Directive on Privacy and Electronic Communications requires Member States to enact laws requiring Internet service providers to utilize appropriate security safeguards on their services and to ensure the confidentiality of the communications.[83]

In addition, the Directive on Privacy and Electronic Communications places strict limitations on the collection of location data, other than traffic data, from cell phones and other portable electronic devices.[84] These limitations include requiring either anonymity with respect to location data or consent by the user or subscriber, which can be withdrawn at any time.[85] Before obtaining consent, the service provider is required to inform the user or subscriber of the type of location data that will be processed, the purpose and duration of the processing, and whether the data will be transmitted to a third party.[86]

---

79. *See id.*

80. *See id.*

81. Directive on Privacy and Electronic Communications, Council Directive 2002/58, 2002 O.J. (L201) 37, 38 (EC), *available at* http://mineco.fgov.be/internet_observatory/pdf/ [hereinafter Directive on Privacy & Electronic Communication].

82. *See id.*

83. *See id.* arts. 4 & 5.

84. *See id.* art. 9.

85. *See id.*

86. *See* Directive on Privacy & Electronic Communication, *supra* note 81.

6. European Commission Staff Working Document: Early Challenges Regarding the "Internet of Things"

In late 2008, the European Commission initiated a public dialogue with respect to the implications of the eventual integration of data from radio frequency identification (RFID) technology into an Internet based amalgamation of electronic data known as the "Internet of Things."[87]

In a draft Commission Staff Working Document entitled "Early Challenges regarding the 'Internet of Things,'"[88] privacy, data protection, and security were cited as some of the public policy challenges resulting from the development and application of RFID technology. After the European Commission has received and studied comments responding to the working document, it intends to issue a Commission Communication to the European Parliament on the Internet of Things in 2009. In recognition of the regulatory challenges that result from the speed of technological innovation, the draft document recommends the development of privacy and security friendly RFID architecture as an initial step prior to consideration of additional regulation.[89] The European Commission's examination of the privacy implications of RFID technology comes at the same time as scholars continue to express concerns about the potential adverse impact that RFID technology may have on human rights.[90]

---

87. As will be seen in Part VI.D. *infra*, the Article 29 Working Party addressed the privacy implications of RFID technology in the workplace in a 2005 opinion. In addition, the European Commission, in 2007, issued a Communication to the European Parliament, entitled "Radio Frequency Identification (RFID) in Europe: steps towards a policy framework" with respect to public policy issues stemming from RFID technology. The Communication is available at http://www.iot-visitthefuture.eu/fileadmin/documents/roleofeuropeancommision/Communication_on_RFID_European_Commission_2007.pdf.

88. Commission of the European Communities, Commission Staff Working Document, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *available at* http://ec.europa.eu/information_society/policy/rfid/documents/earlychallengesIOT.pdf.

89. *Id.* at 8.

90. *RFID Chips: A Privacy and Security Pandora's Box?*, SCI. DAILY, Nov. 28, 2008, http://www.sciencedaily.com/releases/2008/11/081118141854.htm (discussing a recent article by Eleni Kosta and Jos Dumortier from the Interdisciplinary Centre for Law and Information & Communication Technology at the Katholieke Universiteit in Belgium published in the International Journal of Intellectual Property Management about the potential adverse impact on privacy resulting from the implementation of RFID technology).

D. *The Charter of Fundamental Rights*

In December 2000, the leaders of the European Parliament, the Council of Europe, and the European Commission signed, and proclaimed the Charter of Fundamental Rights[91] (Charter). The Charter guarantees, as fundamental rights, the right to privacy and a right of protection for personal data.[92] The Charter was inspired by the ECHR and contains similar, but not identical, provisions with respect to privacy. Pursuant to Article 52 of the Charter, the rights granted by the Charter, which correspond with rights guaranteed by the ECHR, are to be interpreted consistent with the ECHR.[93]

Article 7 of the Charter provides: "Everyone has the right to respect for his or her private and family life, home and communications."[94] Article 7 utilizes the identical wording contained in ECHR, Article 8, section 1, but substitutes the term "correspondence" with the broader term "communications" reflecting the significant growth in electronic documents.[95]

Like the Privacy Directive, the Charter contains explicit privacy protections for personal data and mandates that each country establish a governmental body with the authority to enforce those protections.[96] Article 8 of the Charter states:

> Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.[97]

Although the Charter grants countries permission to establish exceptions to the rights guaranteed by Articles 7 and 8, such exceptions are subject to strict scrutiny.[98] Pursuant to Article 52, these national exceptions must be provided by law and must respect the essence of those

---

91. Charter of Fundamental Rights of the European Union, 200/C, 2000 O.J. (C364) 1 (EC), *available at* http://www.europarl.europa.eu/charter/pdf/text_en.pdf [hereinafter EU Charter].

92. *See id.* at 10.

93. *See id.* at 21.

94. *Id.* at 10.

95. *Compare id., with supra* note 30 and accompanying text.

96. *See* EU Charter, *supra* note 91, at 10.

97. *Id.*

98. *See id.* at 21.

rights.[99] Moreover, such exceptions are subject to the principle of proportionality and codified limitations may be applied "only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others."[100]

The combination of the ECHR, the Privacy Directive, and the Charter establish a firm foundation for the protection of employee privacy in the workplace in Europe. This Article turns next to relevant decisions issued by the European Court of Human Rights interpreting the ECHR.

III. RELEVANT DECISIONS BY THE EUROPEAN COURT OF HUMAN RIGHTS

The European Court of Human Rights has issued a series of decisions interpreting the scope of privacy protections under ECHR, Article 8. These decisions constitute important precedent in the development of European privacy law under the Privacy Directive and in litigation under privacy provisions contained in national legislation.

The scope of ECHR, Article 8 privacy protections is illustrated by a decision from the European Court of Human Rights in a privacy claim brought by a private German attorney, finding that his privacy rights were violated when the local police searched his law office consistent with an order issued by a Munich judge.[101]

In *Niemietz v. Germany*,[102] a local judge received a letter signed with a pseudonym on behalf of an anti-clerical group affiliated with a political party.[103] The letter criticized a pending criminal prosecution of a private employer for refusing to deduct a Church tax from the wages of his employees.[104] In addition, the letter accused the presiding judge of being both biased and incompetent.[105] The resultant criminal investigation into the insulting letter led the German police to obtain a court order directing a search of Niemietz's office as part of an effort by the police to learn the identity of the letter writer.[106] Niemietz was targeted for the search based upon his known affiliation with both the anti-clerical group and the related

99. *See id.*
100. *Id.*
101. *See* Niemietz v. Germany, 16 Eur. Ct. H.R. 97 (1992).
102. 16 Eur. Ct. H.R. 97 (1992).
103. *See id.* ¶ 7.
104. *See id.*
105. *See id.*
106. *See id.* ¶¶ 9-10.

political party.[107] In November 1986, the police conducted a search of Niemietz's law office, pursuant to the court order, including examining his client's files, but found no relevant documents.[108]

Niemietz challenged the search under ECHR, Article 8, Section 1 and it was ultimately heard by the European Court of Human Rights.[109] In sustaining Niemietz's Article 8 arguments, the court made a number of important findings underscoring the scope of ECHR privacy protections.[110]

First, the court rejected Germany's argument that the search of a private law office is not covered under Article 8.[111] Germany claimed that Article 8 only prohibits interference in "private and family life," and "home and correspondence."[112] Although the court found that the search interfered with the attorney's private life, it acknowledged a difficulty in articulating a comprehensive definition of what constitutes a "private life" under ECHR, Article 8.[113] Nevertheless, the court recognized that, in general, the protection of "private life" must include, to some degree, a "right to establish and develop relationships with other human beings."[114] Furthermore, it concluded that an exclusion of professional or business activities from the definition of "personal life" is inconsistent with two practical realities: (a) professional and business activities play a major part in developing personal relationships; and (b) it is very difficult to draw distinctions between an individual's personal activities and professional or business life.[115]

---

107. *See Niemietz*, 16 Eur. Ct. H.R. ¶ 8.
108. *See id.* ¶ 11.
109. *See id.* ¶¶ 23-25.
110. *See id.*
111. *See id.* ¶¶ 27, 29.
112. *Niemietz*, 16 Cur. Ct. H.R. ¶¶ 26-29.
113. *Id.* ¶ 29.
114. *Id.*
115. *See id.* When the Article 29 Working Party prepared Opinion 8/2001 on the processing of personal data in the workplace, it relied on the following quote from ECHR:

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

The court also found that the search interfered with Niemietz's "home."[116] In reaching this conclusion, the court noted that various Member States, including Germany, treated business premises as a home for purposes of Article 8.[117] In addition, the Court cited to the fact that:

> In this context also, it may not always be possible to draw precise distinctions, since activities which are related to a profession or business may well be conducted from a person's private residence and activities which are not so related may well be carried on in an office or commercial premises.[118]

After concluding that the search interfered with rights guaranteed by Article 8, section 1, the court then examined whether the interference was permissible under Article 8, section 2.[119] In perhaps the most significant portion of the decision, the court concluded that the search conducted pursuant to a judicially ordered subpoena constituted interference that was not "necessary in a democratic society."[120] This conclusion was premised on the overly broad scope of the subpoena in comparison to the purpose of the search of the law office: learning the identity of the letter writer.[121] Under the circumstances, the court found that the search of the law office was disproportionate to its purpose because it involved the encroachment into professional secrecy and the potential interference in the administration of justice.[122]

The application of the principle of proportionality in *Niemietz* and under the Privacy Directive, in determining whether there has been a privacy violation, has not been explicitly adopted in American jurisprudence. However, the U.S. Supreme Court has stated that when determining the reasonableness of a search under the Fourth Amendment,[123] a court must apply a balancing test that will "consider the scope of the particular intrusion, the manner in which it is conducted, the justification for initiating it, and the place in which it is conducted."[124]

Opinion of Working Party, at 7, WP (2001) 48 final (Sept. 13, 2001), *available at* http://www.garanteprivacy.it/garante/document?ID=1365969 (quoting ECHR, *supra* note 30, ¶ 29).

116. *See Niemietz*, 16 Eur. Ct. H.R. ¶¶ 31, 33.

117. *See id.* ¶ 30.

118. *See id.*

119. *See id.* ¶ 36.

120. *See id.* ¶¶ 36-38.

121. *See Niemietz*, 16 Eur. Ct. H.R. ¶¶ 36-38.

122. *See id.* ¶ 37.

123. Bell v. Wolfish, 441 U.S. 520, 559 (1979).

124. *See id.* at 998.

In *S. and Marper v. the United Kingdom*,[125] the court recently held that the United Kingdom violated Article 8 by refusing a request, by two British nationals, for the destruction of their cellular samples, DNA profiles and fingerprints after criminal charges against them had been discontinued. The court concluded that:

> the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offenses, as applied in the case of the present applicants, fails to strike a fair balance between competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applications' right to respect for private life and cannot be regarded as necessary in a democratic society.[126]

The court's conclusion with respect to the retention of cellular samples is premised upon its recognition that such samples contain highly sensitive personal information about an individual's health. In many ways, the ruling is consistent with the public policy underlying the enactment of GINA in the United States. With respect to the court's ruling on the retention of DNA samples, the Ninth Circuit has indicated a somewhat similar conclusion under the Fourth Amendment.[127]

In 1997, the European Court of Human Rights examined the application of ECHR, Article 8, to employee workplace privacy. In *Halford v. United Kingdom*,[128] the court ruled in favor of a privacy claim brought pursuant to Article 8 by Alison Halford, a female Assistant Chief Constable employed in the Merseyside Police Authority.[129] Halford, the most senior ranking female police officer in the United Kingdom, filed a gender discrimination claim after her eighth application for a promotion to Deputy Chief Constable within the Merseyside police was rejected.[130] In response to the filing of her discrimination claim, she was subjected to

---

125. [2008] ECHR 1581, *available at* http://www.bailii.org/eu/cases/ECHR/2008/1581.html.

126. *Id.* ¶ 125.

127. United States v. Kincade, 379 F.3d 813, 835-36 n.31 (9th Cir. 2004).

128. *See id.* n.35. In contrast, the European Court of Human Rights' ruling with respect to the expungement of the fingerprints is inconsistent with U.S. precedent. *See* United States v. Schnitzer, 567 F.2d 536 (2d Cir. 1977).

129. 24 Eur. Ct. H.R. 523 ¶ 9.

130. *Id.* ¶¶ 9-10.

various retaliatory acts which included disciplinary measures and the interception of telephone calls for the purpose of gathering negative information about her discrimination claim.[131] Ultimately, Halford's gender discrimination claim was resolved.[132]

Thereafter, Halford commenced a claim under ECHR, Article 8, alleging that her privacy rights were violated when her office and home telephone calls were intercepted.[133] After examining the evidence, the court concluded that there was sufficient evidence to establish that there was a "reasonable likelihood" that Halford's office telephone calls had been intercepted, but the court reached a different conclusion with respect to her home telephone calls.[134] It then proceeded to examine whether the surveillance of Halford's workplace telephone calls violated Article 8.[135]

Halford worked in a private office with two telephones.[136] One phone was designated for her own private use and was connected to the police's internal telephone network.[137] The department did not place any restrictions on her use of the telephones and Halford was granted explicit permission to work on her case during work hours.[138]

Like Germany's unsuccessful argument in the *Niemietz* case, the United Kingdom asserted that Halford's telephone calls did not constitute "private life" and "correspondence" under ECHR, Article 8, section 1.[139] The court rejected this argument, citing earlier precedent holding that telephone calls from a business premises can fall under the rubrics of "private life" and "correspondence" under Article 8.[140] The court also rejected the argument that Halford lacked a "reasonable expectation of privacy" in her workplace.[141] In reaching its decision, the court considered that Halford had not received a warning that her calls were subject to interception; that the two office telephones were for her sole use, with one specifically designated for private calls; and that she had been given assurances that she could utilize her office telephones for her discrimination claim.[142]

---

131. *Id.* ¶ 12.
132. *Id.* ¶¶ 13-15.
133. *Halford*, 24 Eur. Ct. H.R. ¶ 41.
134. *Id.* ¶ 17.
135. *Id.* ¶ 46.
136. *Id.* ¶ 16.
137. *Id.*
138. *Halford*, 24 Eur. Ct. H.R. ¶ 16.
139. *Id.* ¶ 43.
140. *Id.* ¶ 44.
141. *Id.* ¶ 45.
142. *Id.*

The court's adoption and application of the reasonable expectation of privacy standard in *Halford* suggests that the court borrowed a privacy standard from U.S. Supreme Court precedent in the area of workplace privacy. In *O'Connor v. Ortega*,[143] the U.S. Supreme Court applied the same standard in determining whether the search of a public employee's office violated the Fourth Amendment of the U.S. Constitution. Like the court in *Halford*, the U.S. Supreme Court in *O'Connor* concluded that the employee had a reasonable expectation of privacy in portions of his office desk and file cabinet because the employer had failed to establish a policy or practice that discouraged employees from utilizing the workplace for personal purposes.[144]

Privacy decisions under ECHR are also impacting decisions by the U.S. Supreme Court. For example, the majority in *Lawrence v. Texas*[145] held that a Texas sodomy statute was unconstitutional because it infringed on the right to engage in intimate sexual conduct in one's home, citing to various European Court of Human Rights opinions that had declined to follow an earlier contrary U.S. Supreme Court decision.[146] However, reliance on international law in interpreting the U.S. Constitution remains the subject of a spirited debate. For example, in *Lawrence,* Justice Scalia criticized the majority's reliance on the law of foreign nations in determining constitutional rights.[147]

In 2002, the Article 29 Working Group issued a working document with respect to workplace privacy interpreting *Halford, Niemtiz,* and other judicial precedent as recognizing the following principles under ECHR, Article 8:

(a) Workers have a legitimate expectation of privacy at the workplace, which is not 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 workers [sic] legitimate expectation of privacy.

(b) The general principle of secrecy of correspondence covers communications at the workplace. This is likely to include electronic email related files and attached thereto.

---

143. 480 U.S. 709 (1987).
144. *Id.* at 719.
145. 539 U.S. 558 (2003).
146. *Id.* at 576 (majority opinion).
147. *Id.* at 598 (Scalia, J., dissenting).

> (c) Respect for private life also includes to a certain degree the right to establish and develop relationship 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.[148]

In 2007, the European Court of Human Rights was called upon to determine whether an employer's surveillance of workplace e-mail and Internet usage constituted a violation of ECHR, Article 8. In *Copland v. United Kingdom*,[149] the court held that the United Kingdom violated an employee's Article 8 rights by engaging in surveillance of the employee's use of workplace e-mail, the Internet, and telephone.[150] Relying on *Halford*, the court concluded that the employee had a reasonable expectation of privacy in her e-mail, Internet, and telephone use because she had not been given a warning that such usage was subject to monitoring.[151] Furthermore, the court found that the interference was not "in accordance with the law" pursuant to ECHR, Article 8, section 2.[152]

In *dicta*, however, the court indicated that under certain factual circumstances, it may find that the surveillance of an employee's use of e-mail, Internet, or telephone at the place of work is "necessary in a democratic society," where the surveillance is in pursuit of a legitimate aim.[153]

As noted *supra* the Article 29 Working Party will follow precedent interpreting ECHR provisions when examining workplace privacy issues under the Privacy Directive. The article next turns to those opinions and working documents by the Article 29 Working Party which provide relevant guidance with respect to electronic privacy in the workplace.

---

148. Article 29-Data Protection Working Party, Working Document on the Surveillance of Electronic Communications in the Workplace 9-10 (2002), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_en.pdf [hereinafter Article 29 Working Party 2002 document]. For an analysis of U.S. law with respect to surveillance of electronic communications in the workplace, see William A. Herbert, *The Electronic Workplace: To Live Outside the Law You Must be Honest* 12 EMPLOYEE RTS. & EMP. POL'Y J. 49 (2008).

149. 45 Eur. Ct. H.R. 253 (2007).

150. *Id.* ¶ 44.

151. *Id.* ¶¶ 41-42.

152. *Id.* ¶ 48.

153. *Id.*

IV. ARTICLE 29 WORKING PARTY OPINIONS AND WORKING DOCUMENTS

Since its establishment, the Article 29 Working Party has played an instrumental international role in examining the privacy implications of new technologies through its issuance of opinions and working documents.

A. *Opinion on the Processing of Personal Data in Employment*

On September 13, 2001, the Article 29 Working Party issued Opinion 8/2001 dealing with the applicability of the Privacy Directive to the processing of personal information in the employment context.[154] The opinion provides significant guidance relating to employer handling of personal employee data.[155]

The Article 29 Working Party opinion articulates fundamental principles applicable to workplace data protections in Member States.[156] The opinion imposes a balanced approach to the interests of employers and employees with respect to the issue of workplace privacy. This balance stems from the European view that privacy is a component of human dignity, rather than a legal concept shaped by property law and rights.

As part of its introduction to the fundamental principles, the Article 29 Working Party described the central premises of those principles:

> Workers do not leave their right to privacy at the door of their workplace every morning. However, privacy is not an absolute right. It needs to be balanced with other legitimate interests or rights or freedoms. This also applies to the employment context.
>
> Workers, as long as they form part of an organization, have to accept a certain degree of intrusion in their privacy and they must share certain personal information with the employer. The employer has a legitimate interest in processing personal data of his workers for lawful and legitimate purposes that are necessary for the normal development of the employment relationship and the business operation.[157]

---

154. Article 29-Working Party, Opinion 8/2001 (Sept. 13, 2001), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp48en.pdf [hereinafter Opinion 8/2001].

155. *See generally id.*

156. *See generally id.*

157. *Id.* at 19.

Within the context of these central premises, the opinion articulates seven principles applicable to the employment context under the Privacy Directive: finality; transparency; legitimacy; proportionality; accuracy and retention of the data; security; and awareness of staff.[158] The three most significant principles articulated in the opinion are finality, transparency, and proportionality.

Finality requires that an employer utilize the data only for a specified, explicit, and legitimate purpose.[159] Transparency requires that each employee be properly informed about what data is being collected, the purpose of the data collection, and be permitted access to his or her personal data pursuant to Article 12 of the Privacy Directive.[160] Proportionality requires that an employer gather and distribute the information through the least intrusive means by ensuring that the information collected is adequate, relevant, and not in excess of the purposes for which it was gathered.[161]

Opinion 8/2001 explicitly found the Privacy Directive's principles and limitations to be fully applicable to employer workplace monitoring and surveillance of e-mail and Internet use, employee location, employer video surveillance, and the processing of sound and image data in employment.[162] Such monitoring must constitute a proportionate employer response to risks that it faces, taking into account legitimate employee privacy needs.[163] The information collected during the course of the monitoring must be adequate, relevant, and not in excess of the purposes justifying the monitoring.[164] Consistent with transparency, employees must be informed of the existence of the surveillance, as well as the purposes for which the personal data is being processed.[165]

In general, employee consent is not necessary in the employment context as long as other requirements of the Privacy Directive are satisfied.[166] However, explicit employee consent is required when processing sensitive data that reveals an employee's race, ethnicity, religion, political opinions, philosophical beliefs, union membership, health, or sex life.[167]

---

158. *Id.* at 3-4.
159. Opinion 8/2001, *supra* note 154, at 3-4.
160. *Id.*
161. *Id.*
162. *Id.* at 13.
163. *Id.* at 4.
164. Opinion 8/2001, *supra* note 154, at 4.
165. *Id.* at 3.
166. *Id.*
167. *Id.* at 16-17.

In defining what constitutes legitimate employee consent, the Article 29 Working Party applies a standard requiring employee free choice.[168] Unlike the United States, where an employer may impose consent as a pre-condition to employment, the Article 29 Working Party concluded that if an employer makes it impossible for an employee to refuse, it does not constitute consent.[169] The opinion expressly states:

> The Article 29 Working Party takes 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 legitimise 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.[170]

B. *Working Document on Surveillance of Workplace Electronic Communications*

In May 2002, the Article 29 Working Party issued a working document, providing guidance as to the scope of permissible surveillance of workplace electronic communications.[171] The working document supplements Opinion 8/2001 with respect to workplace electronic surveillance and continues the balanced approach espoused by that opinion. It recommends various steps aimed at avoiding encroachment into the privacy of personal e-mail and Internet use by suggesting that employers offer employees private e-mail accounts and use blocking software to stop employees from accessing non-work related web sites.[172]

In drafting the guidelines, the Article 29 Working Party subgroup examined precedent interpreting ECHR, Article 8, including *Halford v. United Kingdom*,[173] as well as other international legal documents relating to privacy. The document concludes that electronic communications utilizing an employer's property are covered by the notions of a "private life" and "correspondence" under ECHR, Article 8.[174]

The working document guidelines set forth the general principles applicable to employer surveillance of employee e-mail and Internet use:

---

168. *Id.* at 3, 23.
169. Opinion 8/2001, *supra* note 154, at 23.
170. *Id.* at 24.
171. Article 29 Working Party 2002 document, *supra* note 148.
172. *See generally id.*
173. *See supra* text accompanying notes 128-32.
174. Article 29 Working Party 2002 document, *supra* note 148, at 10.

(a) necessity; (b) finality; (c) transparency, including notifying the subject of the surveillance; (d) notifying the supervisory authority before carrying out automatic surveillance; (e) providing employee access to the fruit of the surveillance; (f) legitimacy; (g) proportionality; (h) accuracy and retention of the data; (i) security; and (j) awareness of staff.[175]

Under the necessity principle, before engaging in e-mail and Internet monitoring, an employer is obligated to determine that electronic surveillance is "absolutely necessary," after it has examined other less intrusive traditional means of supervision, and determined that they are inadequate.[176] Only in "exceptional circumstances," will electronic surveillance be considered necessary.[177] Examples of "exceptional circumstances" include when an employer has a suspicion that an employee is engaging in criminal activity or when the monitoring is aimed at detecting computer viruses.[178]

Consistent with the transparency principle, an employer must be open and notorious when it comes to electronic surveillance.[179] Covert e-mail monitoring is explicitly prohibited unless permitted by a Member State's law in accordance with the Privacy Directive, such as where specific criminal activity has been identified.[180]

The transparency principle requires an employer to provide employees with an accessible, clear, and accurate statement of the policy regarding e-mail and Internet monitoring.[181] This statement should set forth the employer's computer use policy with respect to employee personal or private communications, the specific reasons and purposes for any surveillance, the details of the surveillance measures, and the employer's enforcement procedures when the employer believes that an employee has violated the computer use policy.[182]

The transparency guidelines further recommend that employers, as a matter of practice, inform or consult with appropriate union representatives before imposing a computer use policy.[183] The guidelines note that collective bargaining can be a useful means in the development

175. *Id.* at 13-19.
176. *Id.* at 13.
177. *Id.*
178. *Id.* at 13-14.
179. Article 29 Working Party 2002 document, *supra* note 148, at 14.
180. *Id.*
181. *Id.* at 14.
182. *Id.* at 14-15.
183. *Id.* at 15.

of a computer use policy that assures proportionality in any electronic monitoring that may be absolutely necessary.[184]

The proportionality principle requires that the surveillance be adequate, relevant, and not excessive in achieving the specified purpose.[185] The surveillance under a computer use policy must be narrowly applied to meet the degree and type of risk facing the company. Therefore, blanket employer monitoring of individual e-mails and Internet wandering, other than when necessary for the system's security, is prohibited.

The Article 29 Working Party encourages, in the context of proportionality, that e-mail monitoring be limited to keeping track of the time and participants to an e-mail, rather than e-mail content.[186] If access to e-mail content is absolutely necessary, employers should take necessary steps to protect the privacy of the communication outside the organization.

C. *Working Document on Biometrics*

On August 1, 2003, the Article 29 Working Party issued a working document on biometrics.[187] Biometrics is an identification technology that examines unique physical characteristics of an individual, such as a fingerprint image, hand or facial geometrics, verbal communication, or iris characteristics.[188] The Article 29 Working Party takes the position that most biometric data is subject to the data protection principles set forth in the Privacy Directive.[189] For access control purposes, it favors the use of biometric systems that use physical characteristics which do not leave traces, such as the shape of a hand, as opposed to fingerprints.[190]

In discussing the applicability of the Privacy Directive's principles to biometric information, the Article 29 Working Party concludes that such data can be used only as long as there has been a strict assessment of the necessity and proportionality for use of biometric data.[191] For example, if biometric information is being processed for the purpose of controlling

---

184. Article 29 Working Party 2002 document, *supra* note 148, at 15.

185. *Id.* at 17.

186. *Id.* at 18-19.

187. Article 29-Data Protection Working Party, Working Document on Biometrics, *available at* http://www.statewatch.org/news/2004/feb/biometric-wp80_en.pdf [hereinafter Article 29 Working Party 2003 document].

188. *See generally* William A. Herbert, *No Direction Home: Will the Law Keep Pace with Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery?*, 2 I/S J.L. & POL'Y 409, 412 n.9 (2006) [hereinafter Herbert, *No Direction Home*].

189. Article 29 Working Party 2003 document, *supra* note 187, at 5.

190. *Id.* at 6.

191. *Id.* at 6-7.

access to a worksite, the use of the same data to analyze an employee's emotional state would be inconsistent with its original purpose.[192] Notably, the document cites to a decision by Portugal's supervising authority prohibiting a university from using a biometric fingerprint system to control and monitor staff time and attendance.[193]

D. *Opinion on the Use of Employee Location Data*

In November 2005, the Article 29 Working Party issued an opinion applying the Privacy Directive principles to the collection of employee location data by an employer utilizing new technologies, such as a global positioning system (GPS),[194] RFID,[195] and cell phones.[196] This conclusion is equally applicable to location data of an individual employee and the location of an assigned vehicle or portable location device.[197] Therefore, the principles of finality, transparency, legitimacy, proportionality, accuracy and retention of data, security and awareness of staff are all applicable to employee location data.

The Article 29 Working Party identified two primary issues with respect to employer use of human tracking technologies: the illusive line between work and private life and the degree of monitoring and surveillance that is acceptable.[198] The opinion concludes that the processing of location data of employees must correspond to a specific employer need.[199] One example of a specific need is when the location data is gathered in conjunction with the transportation of people or goods

---

192. *Id.* at 7.

193. *See* BIOMETRICS IN EUROPE, TREND REPORT (2006), *available at* http://www.libertysecurity.org/IMG/pdf/Trend_Report_2006.pdf (prepared by the European Biometrics Portal) (providing a comprehensive discussion about the use of biometrics in the European Union).

194. *See generally* Herbert, *No Direction Home*, *supra* note 188, at 411 n.6. GPS is a satellite based location tracking technology which can provide an employer with precise real time location data of an employee and employer-owned property through a GPS receiver installed in a hand-held device or attached to a vehicle.

195. *See generally id.* at 412 n.7. RFID is a radio-based identification system that uses tags or cards containing microchips that can be read and thereby track the movement of an object or individual. *Id.*

196. *See* Article 29-Working Party Opinion on the Use of Location Data With a View to Providing Value Added Services 9 (2005), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf [hereinafter Article 29 Working Party 2005 document].

197. *Id.* at 10.

198. *Id.*

199. *Id.*

or is aimed at improving the distribution of resources.[200] In contrast, the gathering of location data would be deemed excessive in situations where an employee is free to organize his or her own travel arrangements or where the monitoring can be accomplished through less intrusive means.[201] Further, the opinion emphasizes that it would be inappropriate for an employer to collect location data for periods when an employee is not working and recommends that all vehicles with tracking equipment should enable an employee to switch off the location function.[202]

The scope of location privacy protections, under the Article 29 Working Party opinion, is much greater than that provided by the current laws in the United States.[203] With the exception of states that have outlawed mandatory implants containing location tracking technologies, there are few legal restrictions in the United States relating to employee location privacy.[204] In Wisconsin, it is a criminal offense to mandate that someone undergo the implant of a microchip;[205] similarly, North Dakota has codified a criminal prohibition against mandatory RFID implants.[206] Nevertheless, the substantive narrowness of these prohibitions is striking when they are compared to the principles outlined in the Article 29 Working Party's Opinion on the Use of Employee Location Data.[207]

This Article next turns to legal developments in the United Kingdom, France, and Canada in the area of workplace privacy. Each country has enacted or modified legislation to meet its Privacy Directive obligations. In addition, the supervising authority in each country has issued determinations and recommendations applicable to the workplace.

V. UNITED KINGDOM

Consistent with the Privacy Directive, the United Kingdom enacted the Data Protection Act 1998 (DPA), which regulates the processing of personal data.[208] The DPA identifies eight personal data protection

200. *Id.*

201. Article 29 Working Party 2005 document, *supra* note 196, at 10.

202. *Id.*

203. *Id.* at 10.

204. Herbert, *No Direction Home*, *supra* note 188, at 461-66.

205. WIS. STAT. ANN. § 146.25(1) (West 2008).

206. N.D. CENT. CODE ANN. § 12.1-15-06 (West 2007).

207. *See* Article 29 Working Party document, *supra* note 148.

208. Data Protection Act, 1998, C. 29 (Eng.), *available at* http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1.

principles as being consistent with the Privacy Directive.[209] The DPA requires that:

1. Personal data shall be processed fairly and lawfully consistent with relevant DPA conditions.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country . . . outside the European Economic Area unless that country . . . . ensures an adequate level of protection . . . .[210]

The United Kingdom's supervisory authority is known as the Information Commissioner's Office (ICO).[211] In June 2003, pursuant to DPA, section 51, the ICO promulgated the Employment Practices Code.[212] The Employment Practices Code is an interpretative guide and does not constitute an enforceable regulatory framework.[213] However, it may be utilized by the ICO when bringing enforcement proceedings under the DPA. The Employment Practices Code's primary aim is to provide

209. *Id.* sched. 1.

210. *Id.*

211. *Id.*

212. Employment Practices Code, http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/coi_html/english/employment_practices_code/about_the_code.html (last visited Nov. 11, 2008).

213. *Id.*

guidance and recommendations to employers about the means of complying with the DPA.[214]

Part 3 of the Employment Practices Code sets forth the ICO's guidance and recommendations regarding the application of the DPA to the implementation of employer monitoring.[215] To ensure compliance with the DPA, the ICO recommends that before implementing a monitoring system, an employer should conduct an adverse impact assessment for the purpose of establishing a balanced program that factors in both the employer's business needs and the employee privacy interests.[216]

The ICO identifies certain core principles that must be examined to ensure a balanced approach to employee monitoring.[217] These principles include employer recognition that employees have a legitimate expectation to a degree of privacy in the workplace and that monitoring usually will intrude on the private lives of employees.[218] Before implementing any form of monitoring, the ICO recommends that employers fully examine the purpose for the monitoring and chose the level of monitoring that is justified for that purpose.[219] In addition, it recommends that employers inform employees of the nature, extent, and rationale for any monitoring except in exceptional situations.[220]

The ICO recommends that an employer's adverse impact assessment contain five steps:

1. Identification of the purpose(s) behind the proposed monitoring and the potential benefits of such monitoring.

2. Identification of any likely adverse consequences that can result from the monitoring including: (a) the extent of intrusion into the private lives of employees with the recognition that the private lives of employees usually extend into the workplace; (b) whether employees will have knowledge of the monitoring and therefore be able to act to limit any intrusion on their privacy; (c) whether the monitoring will adversely impact employee morale thereby

214. *Id.*

215. *Id.*

216. Employment Practices Code, http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/coi_html/english/employment_practices_code/part_3-monitoring_at_work_1.html (last visited Nov. 11, 2008).

217. *Id.*

218. *Id.*

219. *Id.*

220. *Id.*

disrupting the employer-employee relationship and the employee-union relationship; and (d) whether monitoring will impact professional obligations of confidentiality.

3. Consideration of alternatives to monitoring or the application of different methods to satisfy the same purpose as a means of insuring proportionality. Such considerations can include: (a) implementation of improved direct supervision, effective training and clear communications rather than implementing electronic or other systematic forms of monitoring and targeting the monitoring only to specific employees who are suspected of engaging in misconduct.

4. Recognition and taking into account the employer's obligations to provide employees with notice of the monitoring and access to the personal data.

5. Determining whether the monitoring is justified. To render this determination, an employer should weigh the following: (a) the benefits of the method of monitoring; (b) alternative methods; (c) the balance between the benefits and the adverse impact; (d) whether the level of intrusion is absolutely necessary; (e) whether the level of intrusion into private lives is justifiable by a risk of serious damage to the employer's enterprise; and (f) whether there has been consultation with the union or the employees themselves.[221]

With respect to monitoring of workplace electronic communications, such as e-mail and use of the Internet, the ICO recommends that employers prepare computer use policies that explain: the circumstances in which an employee may use the employer's equipment for personal purposes; the extent to which private use is allowed; the restrictions on materials that may be viewed on the Internet; the level of permissible personal use when using the employer's computer network while away from the central workplace; and the purpose of the monitoring or surveillance.[222]

---

221. Employment Practices Code, *supra* note 216.
222. *Id.*

In 2000, the United Kingdom enacted the Regulation of Investigatory Powers Act 2000 (RIPA), which sets forth the legal parameters for the interception of electronic communications.[223] Pursuant to RIPA, sections 4(2) and 78(5), the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 were enacted.[224] The regulations identify when it is permissible for an employer to record or monitor employee e-mail and telephone use without consent.[225] Nevertheless, employers remain obligated to comply with the provisions of the DPA.

In addition to domestic law, ECHR, Article 8 also provides a basis for challenging employer surveillance.[226] In *McGowan v. Scottish Water*,[227] a terminated public water company employee, Robert McGowan, argued that his termination was unlawful because his employer violated ECHR, Article 8.[228] The employer became suspicious that McGowan was submitting false timesheets, and thus commenced an investigation.[229] The employer believed that instead of being present at work, McGowan was spending time at his home, which was located a short distance from the plant.[230] Initially, the employer considered installing video surveillance cameras inside the plant but subsequently rejected the idea as impractical.[231] Instead, the employer hired a private investigator who filmed McGowan as he walked between his home and workplace on a public street.[232]

In determining that ECHR, Article 8 was not violated, the Scottish Employment Appeal Tribunal concluded that, although the covert surveillance impacted McGowan's private and family life, the surveillance was proportionate because it was aimed at investigating specific employee misconduct that would constitute a crime.[233] In addition, the tribunal noted

---

223. Regulation of Investigatory Powers Act C. 23 (Eng.), 2000, *available at* http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1.

224. *Id.*

225. *Id.*

226. Convention for the Protection of Human Rights and Fundamental Freedoms (2003), *available at* http://www.echr.coe.int/nr/rdonlyres/d5cc24a7-dc13-4318-b457-Sc9014916d7a/0/englishanglais.pdf

227. 2005 IRLR 167 (2004).

228. *Id.* ¶ 1.

229. *Id.* ¶ 3.

230. *Id.* ¶ 4.

231. *Id.* ¶ 3.

232. McGiowan, 2000 IRLR 167, ¶ 3.

233. *Id.* ¶ 13.

that the employer considered and rejected a more intrusive means of surveillance inside the workplace.[234]

VI. FRANCE

In France, the Loi Informatique et Libertes (LIL) (the Data Protection and Liberties Act) and the Code du Travail (Labour Code) constitute the primary laws applicable to electronic workplace surveillance.[235] The French governmental agency responsible for data privacy protection is the Commission Nationale de l'Infomatique et des Libertes (CNIL).[236]

Under the Data Protection and Liberties Act, employers must comply with the principle of transparency and are required to notify CNIL prior to implementing any form of automatic data collection.[237] In addition, employers must notify employees who are the subject of the data collection and must inform the employees of their right to access the data.[238] The failure to provide proper notice to the CNIL constitutes a criminal offense punishable by imprisonment and a fine.[239]

In addition, Labour Code L. 120-2 mandates the principle of proportionality with respect to all forms of employer monitoring. Under this principle, an employer must have a legitimate objective and must utilize the least intrusive form of monitoring to accomplish that objective. Furthermore, Labour Code L. 121-8 requires prior notice to an employee or job applicant before an employer collects personal information.[240]

---

234. *Id.*

235. WILLIAM KELLER, INTERNATIONAL LABOR AND EMPLOYMENT LAWS 3-16-3-18 (2003). As NYU's Hauser Global Law School Program has noted, obtaining an English translation of French case law and statutes can be problematic. Globalex, Research French Law, http://www.nyulawglobal.org/globalex/France1.htm# Case_--_English. As a result, my discussion of French law, by necessity, is based upon secondary sources.

236. Cyber-Surveillance in the Workplace, CNIL Report (Feb. 5, 2002) (containing various non-binding recommendations), *available at* http://www.cnil.fr/fileadmin/documents/uk/CNIL-cybersurveillance-feb2002-VA.pdf.

237. CNIL has published a decree identified the means for providing it with notification and for requesting a CNIL opinion. Decree No. 2005-1309 of 20 October 2005, as amended, *available at* http://www.cnil.fr/fileadmin/documents/uk/Decree_No_2005-1309.pdf.

238. KELLER, *supra* note 235, at 3-16-3-17.

239. For example, in April 2007, Tyco Healthcare was fined more than $40,000 for failing to comply with CNIL's repeated requests for a more detailed description of the company's employee data collection database. Philip L. Gordon et al., *French Data Protection Authority Fires Warning Shot to U.S. Multinationals: U.S.-Base Employer Fined for Improper Transfer of Employee Data to the U.S.*, LITTLER BLOGS, May 2007, http://www.littler.com/presspublications/Lists/ASAPs/DispAsaps.aspx?id=974&asapType=International%20Employment%20and%20Labor%20Law

240. KELLER, *supra* note 235, at 3-16.

Finally, Labour Code L. 431-2-1 requires that an employer inform and consult with the Works Council prior to implementing a system of technological monitoring.[241] The failure to engage in such consultation is subject to criminal sanctions.[242]

In *Nikon France v. Frederic Onof*,[243] a French appellate court sustained an employee's wrongful termination suit on the grounds that the employer violated the employee's rights under ECHR, Article 8 and French Labour Code L.120-2 when it obtained and read the employee's explicitly labeled personal e-mail stored on its hard drive.[244] In reaching its holding, the French Supreme Court stated:

> 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.[245]

In 2005, the same French appellate court decided *Philippe X v. Cathnet-Science*.[246] In *Philippe X*, the court reversed a judgment in favor of an employer who had terminated an employee for maintaining pornographic images in a computer file marked "personal" on the employer's computer.[247] The appellate court concluded that, in the absence of particular risk or event, an employer cannot access a computer file that an employee has labeled as personal.[248]

This Article next discusses the privacy laws in Canada, the final nation under consideration. Although Canada is not a Member State of the

---

241. *Id.* at 3-16-3-17.

242. *Id.* at 3-17.

243. MATTHEW W. FINKIN, PRIVACY IN EMPLOYMENT LAW ch.5.III(B)(4), at 288-89 (2d ed. 2008).

244. *Id.*

245. Lasprogata et al., *supra* note 27, ¶ 53 (quoting from a translation of *Nikon France v. Frederic Onuf*).

246. Cour de Cassation, Cass.soc., May 17, 2005, Arret No. 1089 FS-P+B+R+1, Pourvoi No. J-03-40.017.

247. Fred H. Cate, *European Court of Human Rights Expands Privacy Protections:* Copland v. United Kingdom, 11 ASIL INSIGHTS, Aug. 6, 2007, *available at* http://www.asil.org/insights070806.cfm.

248. *Id.*

European Union, it has been proactive, on the national and provincial levels, in the field of electronic privacy.

VII. CANADA

In 2000, Canada enacted the Personal Information Protection and Electronic Documents Act (PIPEDA) in direct response to the EU Privacy Directive.[249] PIPEDA establishes legal protections with respect to the collection and use of personal data by employers in the Canadian federally-regulated sector such as telecommunications, banking, aviation, interprovincial or international trucking.[250]

Prior to enacting PIPEDA, Canada had enacted the Federal Privacy Act, which protects the privacy of personal information of employees employed by the Canadian federal government.[251]

In drafting PIPEDA, the Canadian Parliament incorporated, the ten privacy principles established by the Canadian Standards Association in its Model Code for the Protection of Personal Information:

1. Accountability: an organization must designate an individual who is responsible for ensuring compliance with the principles and must create policies and practices to give effect to the principles, including establishing procedures for complaints and inquiries and the training of staff regarding the policies and training.
2. Identifying Purpose: an organization must identify the purpose(s) for collecting the personal information at or before the time of collection of the data and inform the individual of the purpose at or before requesting the information. The collection, use or disclosure of personal information is permitted only for purposes that a reasonable person would consider appropriate in the circumstances.
3. Consent: in general, an individual's knowledge and consent are required for the collection, use and dissemination of personal information. PIPEDA permits

249. PIPEDA, R.S.C., ch. 5 (2000), *available at* http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp.

250. PIPEDA and Provincial Private Sector Privacy Laws, www.privatech.ca/privacy-laws/canada/ (last visited Nov. 9, 2008).

251. Federal Privacy Act, R.S.C. ch. P-21 (1985), *available at* http://laws.justice.gc.ca/en/showdoc/cs/P-21///en?page=1.

consent to be obtained by various means and consent can be withdrawn at any time.

4. Limiting Collection: personal information can be collected only for the purpose(s) necessary identified by the organization and by fair and lawful means. The amount and type of information collected must be proportionate to the purposes identified. Therefore, collection cannot be indiscriminate.
5. Limiting Use, Disclosure, and Retention: the personal information collected cannot be used or disclosed for a purpose other than that originally identified by the organization without the consent of the individual.
6. Accuracy: collected personal information must be as accurate, complete, and up-to-date as is necessary for the purpose(s) for which it is collected and used. Routine updating of personal information is prohibited unless it is necessary to fulfill the purpose(s) for which it is collected.
7. Safeguards: an organization must establish security safeguards to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification.
8. Openness: specific organizational policies and practices with respect to the management of personal information must be both reasonably available and generally understandable.
9. Individual Access: Upon request, an individual is entitled to know the existence, use, and disclosure of his or her personal information; have access to the information; and be allowed to challenge the accuracy and completeness of the information; and have it modified as appropriate.
10. Challenging compliance: Organizations are required to establish procedures for complaints or inquiries relating to the handling of personal information.[252]

Canada has established a federal agency, the Office of the Privacy Commissioner (OPC). The OPC is an independent government office with the power to investigate complaints under PIPEDA and the Federal Privacy Act and to commence court litigation to enforce federal privacy

252. IPEDA, R.S.C., ch. 5, sched. 1, §§ 4.1-4.10.4 (2000).

protections.[253] The OPC also plays an important role in analyzing the privacy implications of new technologies in employment such as biometrics, GPS, and RFID.

In 2004, the OPC dismissed a complaint filed by employees alleging that their privacy rights were violated when an employer required them to provide a biometric voice print for logging work-related information.[254] The purpose of the system was to permit field employees to log in and authenticate themselves in a cost-effective manner.[255] The OPC concluded that the biometric voice print, used solely for an individual employee's authentication, constituted a fairly benign privacy intrusion and satisfied the reasonable purpose requirement under PIEPDA.[256]

Subsequently, the OPC issued a report dismissing a complaint against an employer for using GPS technology. It, however, expressed concerns that data obtained may violate privacy rights when job performance is evaluated based upon employer assumptions stemming from that electronic data.[257] More recently, OPC issued a preliminary consultation paper, entitled Radio Frequency Identification (RFID) in the Workplace: Recommendations for Good Practices, which recommends ten privacy principles applicable to the use of RFID technology in the workplace.[258]

In addition, many Canadian provinces have enacted their own privacy laws applicable to the private sector employment context. Some of these laws create a provisional privacy commissioner with the power to investigate and prosecute complaints of workplace privacy violations and to study and report on privacy issues. For example, British Columbia's Personal Information Protection Act, section 13,[259] defines when a private employer may collect employee personal information. The provision permits employers to collect employee personal information without consent if the "collection is reasonable for the purposes of establishing,

---

253. *Id.* ch. 5, §§ 11-17 (2000); Federal Privacy Act, R.S.C., ch. P-21, § 29 (1985).

254. Commissioner's Findings, PIPEDA Case Summary #281, *Organization Uses Biometrics for Authentication Purposes*, *available at* http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040903_e.asp.

255. *Id.*

256. *Id.*

257. Commissioner's Findings, PIPEDA Case Summary #351, *Use of Personal Information Collected by Global Positioning System Considered*, *available at* http://www.privcom.gc.ca/cf-dc/2006/351_20061109_e. asp.

258. Office of the Privacy Commissioner of Canada, Radio Frequency Identification (RFID) in the Workplace: Recommendations for Good Practices: A Consultation Paper, Mar. 2008, *available at* http://www.privcom.gc.ca/information/pub/rfid_e.asp#Part2.

259. British Columbia's Personal Information Privacy Act, B.C.R. 473, § 13 (2003), *available at* www.qp.gov.bc.ca/statreg/stat/P/03063_01.htm.

managing or terminating an employment relationship between the organization and the individual."[260] However, an employer is required to provide notice to the employee that the information is being collected along with information about the purpose for the collection.[261]

Similarly, Alberta's Personal Information Protection Act, section 15, provides that an employer can collect personal information without individual consent if the individual is an employee or if the information is for the purpose of recruiting a potential employee.[262] However, the collection of personal information about an employee must be reasonable in light of the purpose for which it is being collected and must be related to the employment relationship.[263] Under Alberta law, employees must be given reasonable notification that the information is going to be collected and must be advised of the purpose for the data collection.[264]

VII. CONCLUSION

A review of developments abroad in the area of electronic workplace privacy law demonstrates that the United States is far behind in studying the implications of the technological transformation of the workplace and acting to establish an enforceable balance between respective workplace interests. Despite the ever-widening gap between the public perception and the legal reality of privacy rights in the American workplace, there has been little movement on the federal, state and local levels in this area. The recent enactment of GINA, following years of federal study into the issue of genetic discrimination, is a hopeful sign that the reign of deregulation ideology may be ending.

The lack of American initiative in developing a nuanced approach to workplace privacy in the face of new technologies is strikingly inconsistent with the leadership that the United States has previously provided in the field of privacy. Over a century ago, it was Louis Brandeis and his law partner Samuel Warren who famously advocated in the Harvard Law Review for the recognition of a common law right to privacy.[265] Their article, along with other forces, precipitated some states

---

260. *Id.*

261. *Id.*

262. Alberta's Personal Information Protection Act, A.R., ch. P-65, § 15 (2003).

263. *Id.*

264. *Id.*

265. Samuel L. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). A few decades later, in his dissenting opinion in *Olmstead v. United States*, 277 U.S. 438,

to recognize a common law right to privacy. In our own time, it remains to be seen what will precipitate a meaningful societal discussion aimed at establishing a reasonable legal framework for the contemporary American workplace that balances the respective interests and rights of employers and employees.

As we have seen, the European Union, the United Kingdom, France, and Canada have all moved swiftly to establish legal infrastructures aimed at responding to the privacy implications of the computer-based technological revolution. These infrastructures have resulted in reports, opinions, and decisions that establish similar approaches to privacy issues in the electronic workplace. It is probable that the administrative structures and analyses developed abroad may provide helpful guidance as the United States develops its own public policy that goes beyond its heavy reliance on employer self-regulation.

---

478 (1928), then Justice Brandies argued in favor of a right to privacy emanating from the Fourth Amendment to the U.S. Constitution.