Loyola of Los Angeles International and Comparative Law Review

Volume 31 | Number 2 Article 5

3-1-2009

Copland v. United Kingdom: What is Privacy and How Can Transnational Corporations Account for Differing Interpretations

Frances Ma

Copland v. United Kingdom: What Is Privacy and How Can Transnational Corporations Account for Differing Interpretations?

I. INTRODUCTION

Mr. Jones wakes up at six thirty a.m. to the buzzing sound of his company Blackberry. He presses the snooze button twice and then finally rolls out of bed. Before heading into the shower, he checks his e-mail—the light indicating new messages has been flashing since one o'clock in the morning. Scrolling through his personal Gmail, he finds that his old college buddy has been out on the town again and has sent him a few drunken messages about the woman he's been dating for the past week. Mr. Jones responds to his buddy's messages with an old photo he finds on his blog from college. The photo shows Mr. Jones and his buddy doing keg stands dressed in drag for Halloween. After skipping through a few miscellaneous company e-mails, Mr. Jones hops into the shower and heads to the airport for his flight to England.

While waiting in the terminal, Mr. Jones checks his baseball fantasy stats on ESPN.com. Noticing that his best player, Albert Pujols, is injured for the season, he spends the next thirty minutes before the flight trying to decide which player he can trade to replace Pujols. As the flight begins to board, Mr. Jones remembers to call his brother at work to remind him to feed his dog, Pudge, while he is out on business. His brother works for Alcoholics Anonymous as a counselor, and unfortunately, Mr. Jones has forgotten his brother's direct line, so he calls the hotline and waits until he reaches an attendant that can direct him to his brother. After a two-week business trip in London, Mr. Jones finally returns to the States. The first thing he does is to call his brother to check up on Pudge.

Throughout this time, pursuant to company policy, Mr. Jones' e-mail, phone, and internet activity have been tracked on his Blackberry. The company log indicates that Mr. Jones checked his

email at seven a.m., spent ten minutes reading messages from a sender by the name of "HoTtStUfF"; spent twenty minutes searching through a blog website called "Pretty in Pink"; responded to "HoTtStUfF" with an e-mail containing the subject line, "a night to remember!" with a photo attached; spent two minutes clicking through twenty e-mails sent by the company; surfed the web on ESPN.com for thirty-five minutes; talked to five different users on a fantasy baseball league; and called Alcoholics Anonymous once before leaving the States and once after his return. The log is blank for the two weeks spent in England.

Why the two week gap in e-mail, phone, and internet activity? The explanation lies in the difference between privacy rights in the United States and those in the Member States of the UN Convention for the Protection of Human Rights and Fundamental Freedoms (the Convention). This Note discusses the extent to which the European Court of Human Rights (ECHR) has expanded the privacy rights of individuals, not only within the confines of the home but in the workplace as well, through its decision in *Copland v. United Kingdom*.[1] The disparities in how the two regions collect, use, and retain employee information may have far reaching effects on how United States' businesses choose to operate abroad. The new restrictions on electronic information, more specifically, may have stifling effects on the United States' ability to conduct commerce with European countries.

Part II of this Note discusses how the case of *Copland v. United Kingdom* has expanded privacy rights under the Convention. Part III analyzes the privacy right perspectives of the United States; Part IV analyzes the privacy right perspectives of Europe under the Convention; and Part V discusses how the differences in privacy right perspectives will affect transnational corporations. Finally, Part VI suggests the remedies available for United States corporations that intend to conduct business abroad.

II. THE *COPLAND* CASE

In April 2007, the ECHR found in favor of Ms. Lynette Copland, a UK citizen and a personal assistant to the College Principal at Carmarthenshire College in Wales.[2] The Court determined that Carmarthenshire College had violated Ms.

1. Copland v. United Kingdom, 45 Eur. Ct. H.R. 235 (2007).
2. *Id.* ¶¶ 7, 49.

Copeland's Article 8 privacy rights under the Convention because the college monitored her telephone calls, e-mail, and internet usage without her knowledge.[3]

The surveillance began after Ms. Copland visited another campus of the College with a male director and was assumed to have an "improper relationship" with him.[4] Subsequently, the Deputy Principal of the College approved the monitoring of Ms. Copland's telephone calls.[5] The College began logging the phone numbers she dialed, the dates and times of those phone calls, and the length of each call.[6] From October to November of 1999, the College also monitored Ms. Copland's internet usage by keeping track of the websites she visited, the times and dates of the visits, and the length of time she stayed at each website.[7] Moreover, the College monitored Ms. Copland's e-mails by analyzing the e-mail addresses she used and the dates and times at which the e-mails were sent.[8] The e-mail monitoring lasted roughly six months.[9]

When Ms. Copland learned that her e-mails were being monitored, she contacted the College Principal to inquire about a possible investigation. She was told that although all e-mail activity was tracked, the Deputy Principal had specifically requested her e-mail information to be investigated.[10] Eventually, Ms. Copland learned from other colleagues that several of her activities, beyond just her e-mails, were being monitored.[11] The College claimed that it monitored Ms. Copland's telephone, e-mail, and internet usage in order to ensure that the College's facilities were not being used excessively for personal purposes.[12]

The College asserted that the monitoring was minimal and provided two arguments to justify its actions: (1) the College was attempting to protect "the rights and freedoms of others by ensuring that the facilities provided by a publicly funded employer were not abused" and (2) the College, as a statutory body, had the power to take "reasonable control" of its facilities and to "do

3. *Id.* ¶¶ 39-49.
4. *Id.* ¶ 9.
5. *Id.* ¶ 10.
6. *Id.*
7. *Id.* ¶ 11.
8. *Id.* ¶ 13.
9. *Id.*
10. *Id.* ¶ 12.
11. *Id.* ¶ 16.
12. *Id.* ¶ 34.

anything necessary and expedient" for the purposes of providing further and higher education.[13] While the College monitored Ms. Copland's telephone calls, e-mails, and internet usage, however, it did not have a policy in place regarding the monitoring of such facilities.[14]

The ECHR determined that the United Kingdom was a Member State subject to the rules and regulations of the Convention and that it was directly responsible for the conduct of its public entities such as Carmarthenshire College.[15] Based on Article 8 of the Convention, the court first addressed whether the conduct of the College fell within the purview of the rights established by Article 8. The court then determined whether any interference of the right was "in accordance with the law" or in other words, whether the conduct was in compliance with domestic law.[16]

With respect to the scope of Article 8, the court stated that according to *Halford v. United Kingdom*[17] and *Amann v. Switzerland*,[18] the monitoring of telephone calls alone was *prima facie* covered by Article 8's concept of "private life" and "correspondence" regardless of whether the surveillance took place in the employment context.[19] The court also concluded that the information obtained from surveillance of Ms. Copland's e-mail and internet usage should be treated no differently than the information obtained from the monitoring of her phone calls and therefore, were also covered by Article 8 of the Convention.[20] Moreover, the court found irrelevant the question as to whether the College disclosed the data collected from Ms. Copland, because the act of collecting and storing the information itself was enough to constitute an intervention of Ms. Copland's respect for her private life and correspondence under the Convention.[21] Finally, Ms. Copland had a reasonable expectation of privacy

13. *Id.*
14. *Id.* ¶ 15.
15. *Id.* ¶ 39.
16. *Id.* ¶ 41-49; Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 222 (as amended by Protocol no. 11), *available at* http://conventions.coe.int/treaty/en/Treaties/Word/005.doc [hereinafter The Convention].
17. Halford v. United Kingdom, 24 Eur. Ct. H.R. 523 (1998).
18. Amann v. Switzerland, App. No. 27798/95, 30 Eur. H.R. Rep. 843 (2000).
19. *Copland*, 45 Eur. Ct. H.R. ¶ 41.
20. *Id.*
21. *Id.* ¶ 43.

because she was not given any warning that her phone calls, e-mails, or internet usage would be monitored.[22]

The court was also not convinced by the government's arguments relating to the justification of its actions under domestic law. At the time the acts complained of were committed, there was no general right to privacy under English law.[23] The only domestic law that regulated the manner in which organizations could hold, process, or use data was the Data Protection Act of 1984.[24] According to the "data protection principles" of the Act, "[p]ersonal data held for any purpose shall be adequate, relevant and not excessive in relation to that purpose or those purposes."[25] The Act provided compensation for an individual only if his or her personal data was disclosed improperly.[26] In this case, the government failed to provide any domestic provisions that regulated the circumstances in which employers could monitor the use of telephones, e-mail, or the internet.[27] Additionally, the court was not persuaded that the government had a statutory power to do "anything necessary or expedient" for the purposes of providing higher and further education.[28] Consequently, the government was found to be in violation of Article 8 of the Convention.

The ECHR's decision in *Copland* clearly establishes an expansion of the Convention's Article 8 rights. Now, individuals not only have the right to privacy with respect to their family life, home, and correspondence, but this right extends to any correspondence in the workplace. Employers are therefore obligated to ensure that their employee monitoring policies and procedures comply specifically with domestic and international law.

III. PRIVACY IN THE UNITED STATES

In the United States, privacy is considered a liberty. Although the right to privacy is not explicitly written in the United States

22. *Id.* ¶ 42.
23. *Id.* ¶ 18.
24. *Id.* ¶ 24.
25. *Id.* ¶ 26.
26. *Id.* ¶ 27.
27. *Id.* ¶ 48.
28. *Id.* ¶ 47.

Constitution, its ideals are incorporated into the Bill of Rights.[29] The Fourth Amendment, for example, bans unreasonable searches and seizures and recognizes a person's right to be left alone from government intrusion, especially within the confines of the home.[30] When a person leaves his home, however, the rules regulating privacy change dramatically because an individual, for the most part, sheds his expectation of privacy, especially when he is under the limelight of the media.[31] In the United States, privacy rights are consequently found in a variety of forms; a combination of statutory and common law,[32] through "legislation, regulation, and self regulation."[33] Government intervention is limited and regulation is narrowly tailored to fit specific needs for different types of situations involving privacy rights.[34]

In the employment sector, there currently is no overarching federal law on privacy that applies to the workplace.[35] The rules, therefore, regulating the extent to which employers may monitor or survey its employees vary from state to state. The public perception however, always seems to begin with "Big Brother" from George Orwell's novel, *1984*.[36] As technological advances continue to develop, employers have become even more adept at monitoring the minute details of their employees' work habits and activities.[37] One scholar has even written, "No successful standards, legal or otherwise, exist in the United States for limiting the collection and utilization of personal data in cyberspace."[38] Today,

---

29. *See* U.S. CONST. amends. I-X.

30. *See* U.S. CONST. amend. IV; United States v. Karo, 468 U.S. 705, 714-15 (1984); Welsh v. Wisconsin, 466 U.S. 740, 748-749 (1984); Steagald v. United States, 451 U.S. 204, 211-212 (1981).

31. Bob Sullivan, *'La Difference' Is Stark in EU, U.S. Privacy Laws: EU Citizens Well Protected Against Corporate Intrusion, But Red Tape is Thick*, MSNBC, Oct. 19, 2006, http://www.msnbc.msn.com/id/15221111.

32. *See* Laura Evans, Comment, *Monitoring Technology in the American Workplace: Would Adopting English Privacy Standards Better Balance Employee Privacy and Productivity?*, 95 CAL. L. REV. 1115, 1120 (2007).

33. Safe Harbor Overview, EXPORT PORTAL, http://www.export.gov/safeharbor/eg_main_018236.asp (last visited Apr. 26, 2009).

34. Evans, *supra* note 32. *See, e.g.*, Video Privacy Protection Act, 18 U.S.C. § 2710 (2002); Family Educational Rights and Privacy Act of 1998, 20 U:S.C. § 1232g (1998); Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 (1998).

35. Evans, *supra* note 32, at 1123.

36. CAMILLE HÉRBERT, EMPLOYEE PRIVACY LAW 8A-4 (Thomson West 2007) (1993).

37. *Id.* at 8A-5.

38. PAUL SCHWARTZ, PRIVACY, PARTICIPATION, AND CYBERSPACE: AN AMERICAN PERSPECTIVE, IN ZUR AUTONOMIE DES INDIVIDUUMS 337-38 (2000).

employers most commonly use computers as a method of monitoring.[39] In fact, according to a survey of 110 organizations conducted by the National Institute for Occupational Safety and Health in 1982 to 1984 and again in 1985 to 1986, 80–90 percent of organizations used a computer to monitor the activities of its workers.[40] The Privacy Foundation has reported that 35 percent of workers in the United States are continuously monitored with regard to their e-mail and internet usage.[41] A 2001 American Management Association study also showed that of the large employers surveyed, 80 percent reported that they listened to employee phone conversations and voice mail and monitored electronic files and e-mail.[42] With a computer, an employer can track an employee's break times, the precise time and location a clerical error is made, the number of keystrokes per minutes, the time it takes to complete any task, internet activity such as websites that are visited, how long the employee stays at each site, whether the website is work related or not, and chat rooms that have been entered.[43] A computer can also be used to track specifics on employees who use their phone for sales such as the number of calls that are made, the number of call backs made, the amount of time that passes before the phone is answered, how long a caller is put on hold, and the number of messages on a phone that have yet to be opened.[44] In situations where an employer provides its employees with computers, the employer can also easily view any files or programs that have been downloaded or created on the computer with or without the employee's knowledge.[45]

Some employers justify the use of electronic monitoring and surveillance by explaining that it provides an objective way to evaluate performance levels and provide concrete feedback to its employees regarding performance issues.[46] Others assert that such

39. HÉBERT, *supra* note 36, at 8A-5.

40. *Id.* at 8A-7.

41. Andrew Schulman, *The Extent of Systematic Monitoring of Employee E-mail and Internet Use*, PRIVACY FOUNDATION, July 9, 2001 *available at* http://www.sonic.net/~undoc/extent.htm.

42. American Management Association, *2001 AMA Survey: Workplace Monitoring & Surveillance, Summary of Key Findings*, AMA RESEARCH (2001), *available at* http://www.amanet.org/research/pdfs/emsshort2001.pdf.

43. HÉBERT, *supra* note 36, at 8A-6.

44. *Id.* at 8A-6.

45. *Id.*

46. *Id.* at 8A-17.

measures prevent employees from stealing things or disclosing important company information that should not be released, and yet others explain that measures are put into place to ensure that the company's equipment is being used for business purposes only.[47] American philosophy, in general, has favored the free flow of information and the freedom of contract.[48] "One major aspect of American information privacy culture is its emphasis on classically derived economics, where society is market dominant and rights are political rather than social in nature."[49] Employees are therefore, free to choose where they work, but are not free to dictate how the workplace operates, a choice left to the employer.[50] The freedom of contract allows individuals to waive their privacy rights in exchange for employment.[51]

Although certain limitations are placed on an employer's ability to monitor its employees, the amount of information employers may track is significant. In the United States, the law has not recognized a strong privacy right on the part of employees regarding internet use,[52] and the courts have frequently balanced the scales in favor of the employer.[53] In *O'Conner v. Ortega,* for example, the court discussed the issue of whether an employer's manual search violated an employee's Fourth Amendment right to be free from unreasonable searches and seizures in areas where he or she has a reasonable expectation of privacy.[54] In the end, the court indicated that the existence of a reasonable expectation of privacy in the workplace would depend on the "operational realities of the workplace" and should be decided on a case-by-case basis.[55] In general, the nature of the workplace is such that it is considered to be a public space where an employee is hired for the purpose of completing company business, not private or personal

47. *Id.* at 8A-18.

48. *See* Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1330-31 (2000).

49. Evans, *supra* note 32, at 1138-39.

50. *Id.* at 1139.

51. *Id.*

52. *See* Christopher Pearson Fazekas, Comment, *1984 is Still Fiction: Electronic Monitoring in the Workplace and U.S. Privacy Law*, 2004 DUKE L. & TECH. REV. 15 (2004).

53. Evans, *supra* note 32, at 1122.

54. *See* O'Conner v. Ortega, 480 U.S. 709 (1987).

55. *See id.*

matters.[56] The courts, therefore, tend to reject employee privacy claims on the basis that there is no reasonable expectation of privacy even though no bright line test exists to determine whether an employee should have a reasonable expectation of privacy in certain aspects or areas of his or her job.[57] Moreover, employees have the burden to persuade the judge that the intrusion into their private matters would be "highly offensive" to a reasonable person.[58] In *Smyth v. Pillsbury Co.*, for example, a man sued his employer for terminating his employment on the basis of sending "inappropriate and unprofessional comments" through the employer's e-mail system despite the fact that the employer informed him that his e-mail was confidential.[59] The court there dismissed the case because it found that a reasonable person would not think the interception of e-mail was highly offensive.[60] *Smyth* presents a stark contrast to the conclusions found in *Copland*. It seems certain that if *Copland* had been heard under U.S. privacy laws, the outcome would have been much different.

Most employers are also able to get around a Fourth Amendment claim by establishing that they have a regular scheme or practice of monitoring its employees.[61] Additionally, courts have generally found that if the surveillance is closely related to the integral functions of a job, the employee should not have a reasonable expectation of privacy regarding those functions.[62] Aside from a few limitations, it seems that employers have wide discretion to implement several different forms of monitoring mechanisms as long as a legitimate reason for them exists.[63] In this day and age, it also seems as if people have come to expect that their employers will be tracking their activities either through computers or videotaping devices.

---

56. *See* Joan Gabel & Nancy Mansfield, *The Information Revolution and Its Impact on the Employment Relationship: An Analysis of the Cyberspace Workplace*, 40 AM. BUS. L.J. 301 (2003).

57. *See id.*

58. *See* Fazekas, *supra* note 52.

59. Smyth v. Pillsbury Co., 914 F. Supp. 97, 98 (E.D. Pa. 1996).

60. *Id.* at 101.

61. HÉBERT, *supra* note 36, at 8A-53.

62. *Id.* at 8A-52.

63. ANDREW CLAPHAM, HUMAN RIGHTS IN THE PRIVATE SPHERE 214-25 (1993) ("In the United States a recent survey revealed that companies regularly search cars, lockers, handbags, desks, etc., claiming that the economic risks of high medical costs and suits for 'negligent hiring' necessitate such action to guard against possible alcoholics and drug abusers.") [hereinafter CLAPHAM, PRIVATE SPHERE].

IV. PRIVACY IN EUROPE

In Europe, unlike the United States, an intrusion on privacy is considered an attack on one's dignity, and therefore, is automatically considered an improper violation of one's rights.[64] Most of Europe relies on comprehensive legislation to enforce its ideals behind individual privacy rights.[65] The individual does not generate the privacy right; thus, the right cannot be contracted away as in the United States.[66] The privacy rights in Europe extend far beyond one's home, into the workplace, and even under the attention of the media.[67] Privacy statutes apply broadly to all categories of data, including health information, financial data, and employment records, whereas the American system has specific laws for specific uses of personal data.[68] Moreover, in Europe, the retention of personal information itself, regardless of the reasons behind the retention, can be considered a violation of one's privacy rights.[69] Some experts believe Europe's privacy objectives differ from the United States' because of Europe's unique history, which molded the mentality of its people and how they believe the government should be run.[70] Most European countries, for example, trust their government with personal information, but do not trust private organizations to handle such information.[71] The opposite is true in the United States where people generally do not mind sharing personal information to private organizations, but become weary when the government is at their doorsteps asking for information.[72]

The overarching piece of legislation regulating privacy rights of several European countries is Article 8 of the Convention.[73] Under this provision, each individual country can enforce its own

---

64. Sullivan, *supra* note 31.

65. Safe Harbor Overview, *supra* note 33.

66. Gail Lasprogata et al., *Regulation of Electronic Employee Monitoring: Identifying Privacy Through a Comparative Study of Data Privacy Legislation in the European Union, United States, and Canada*, 2004 STAN. TECH. L. REV. 4, 8 (2004).

67. Resolution on the Protection of Privacy, EUR. PARL. DEB. 24, Doc. No. 1165 (June 26, 1998).

68. Evans, *supra* note 32, at 1130.

69. LOUKIS LOUCAIDES, ESSAYS ON THE DEVELOPING LAW OF HUMAN RIGHTS 97-99 (1995).

70. Sullivan, *supra* note 31.

71. *Id.*

72. *Id.*

73. The Convention, *supra* note 16, at art. 8.

specific laws that will further protect its citizens' privacy rights beyond the stipulations of Article 8.[74]

A. Evolution of Article 8 of the Convention

The Convention for the Protection of Human Rights and Fundamental Freedoms was first drafted by the Council of Europe in 1950 and has been ratified by forty-five European countries.[75] It was intended to incorporate the rights stated in the Universal Declaration of Human Rights[76] and "provid[e] foundations on which to base the defense of human personality against all tyrannies and against all forms of totalitarianism."[77] The original thirteen articles of the Convention enumerate the most basic of individual rights determined by the Council of Europe and apply to every person within a Member State's jurisdiction regardless of nationality.[78] Today they can be found in Articles 2 through 14.[79] Among these rights is Article 8: The right to respect for a private life. Article 8 contains two sections. The first section establishes the scope of the right to a private life and the second section provides limits to this privacy right. It states:

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

---

74. *Id.*

75. Nonnie Shivers, *Firing "Immoral" Public Employees: If Article 8 of the European Convention on Human Rights Protects Employee Privacy Rights, Then Why Can't We?* 21 ARIZ. J. INT'L & COMP. L. 621, 630 (2004) (The countries subject to the Convention are: Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxemborg, the former Yugoslav Republic of Macedonia, Malta, Moldova, Netherlands, Norway, Poland, Portugal, Romania, Russia, San Marino, Serbia and Montenegro, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, and the United Kingdom).

76. YUTAKA ARAI ET AL., THEORY AND PRACTICE OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS 4-5 (Peiter van Dijk et al. eds., Intersentia 4th ed. 2006).

77. FUNDAMENTAL RIGHTS IN EUROPE: THE EUROPEAN CONVENTION ON HUMAN RIGHTS AND ITS MEMBER STATES, 1950-2000, 5 (Robert Blackburn & Jörg Polakiewicz eds., 2001).

78. ARAI ET AL., *supra* note 76, at 13.

79. *Id.* at 8-9.

> the country, for the prevention of disorder or crime, for the protection of heath or morals, or for the protection of the rights and freedoms of others. [80]

The right to respect for one's private life has been interpreted to "[stand] for the sphere of immediate personal autonomy." [81] It is a positive right that is not limited to "'an inner circle' in which the individual may live his own personal life as he chooses and exclude therefrom the outside world not encompassed within this circle, but extends further, comprising to a certain degree the right to establish and develop relationships with other human beings in the outside world." [82] Although Section 1 specifically states that the respect for privacy be applied to "family life, his home and his correspondence," Article 8 has been construed and is confirmed by *Copland* to extend to any correspondence conducted within the workplace. [83]

Section 2 of Article 8 is used to provide public entities with broad discretion regarding the decisions made to limit individual privacy for the interest of the public. [84] *Copland*, however, seems to suggest that any interference of one's privacy rights must be narrowly tailored to fit squarely within the exceptions listed under Section 2. [85] In *Klass v. Germany*, for example, the court found that secret surveillance of telephone calls interfered with Article 8 because it did not fall within the exceptional case of national security. [86] In order to fall within this narrow category, the surveillance must be "specifically reasoned and relevant legislation must provide adequate and effective criteria and other safeguards against its abuse." [87] At the very least, the interference of privacy must be "in accordance with the law." [88] The "law" referred to by the Convention is covered by statutes and unwritten law where the law (1) is "adequately accessible" and (2) is "formulated with

---

80. The Convention, *supra* note 16.

81. KAREN REID, A PRACTITIONER'S GUIDE TO THE EUROPEAN CONVENTION OF HUMAN RIGHTS 323 (1998).

82. *Id.* at 323-24. *See also* Helen Mountfield, *The Implications of the Human Rights Act of 1998 for the Law of Education*, 1 EDUC. L.J. 146 (2000).

83. *See* Orla Ward, *Is Big Browser Watching You?*, 150 NEW L.J. 1414 (2000).

84. Stanley Naismith, *Religion and the European Convention on Human Rights*, 2 HUM. RTS. & U.K. PRAC. (1998).

85. *See also* Cindy Burnes, *Confidence and Data Protections*, *in* 1.2 PRIVACY AND DATA PROTECTION 4 (2000).

86. *See* Klass v. Germany, App. No. 20605/92, 2 Eur. H.R. Rep. 214 (1992).

87. LOUCAIDES, *supra* note 69, at 97.

88. *See* Ward, *supra* note 83.

sufficient precision" such that an individual may be able to foresee a violation and therefore regulate her conduct.[89] In practical terms, the conduct of an entity is "in accordance with the law" if it complies with domestic law.

Hence, Article 8 of the Convention requires not only that the conduct fall within the scope of the established right, but also must be in compliance with domestic laws that are sufficiently clear to give individuals adequate notice of circumstances or conditions in which their rights might be implicated.[90]

B. Other European Privacy Initiatives Implicated by Article 8 of the Convention

Because Section 2 of Article 8 requires any interference with a person's privacy rights to be in compliance with domestic law, it is important to understand the scope and limitations of the privacy rights that have been established by most European countries. Here, this Note attempts to give a brief overview of two of the most widely held privacy acts adopted by Member States of the Convention and additionally, provide an overview on specific regulations that particular Member States have created on their own with respect to employee privacy rights.

1. Data Protection Directive of 1995

In an attempt to harmonize data protection regulation, the European Commission proposed the Data Protection Directive of 1995 (the Directive), which encompasses seven main principles that were first established by the Organization for Economic Cooperation and Development (OECD).[91] In 1980, the OECD issued its *Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data* where it discussed seven main principles.[92] These principles included: (1) Notice—data subject should be given

89. Kruslin v. France, 176-A Eur. Ct. H.R. (ser. A) CD451, 455 (1990). *See also* Malone v. United Kingdom, App. No. 8691/79, 7 Eur. H.R. Rep. at 45 (1984); Khan v. United Kingdom, App. No. 35394/97, 31 Eur. H.R. Rep. 45 (1982).

90. *Copland*, 45 Eur. Ct. H.R. ¶ 46.

91. Organization for Economic Cooperation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Jan. 5, 1999, http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (last visited Apr. 26, 2009).

92. *Id.*

notice when his or her data is being collected, (2) Purpose—data should only be used for the purpose stated and not for any other purposes, (3) Consent—data should not be disclosed without the data subject's consent, (4) Security—collected data should be kept secure from any potential abuses, (5) Disclosure—data subjects should be informed as to who is collecting their data, (6) Access—data subjects should be allowed to access their data and make corrections to any inaccurate data, and (7) Accountability—data subjects should have a method available to them to hold data collectors accountable for following the other six principles.[93] The first Article of Chapter One of the Directive states, for instance, that its purpose is to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[94]

According to the Directive, foreign businesses that wish to transmit personal data of European citizens in Europe must abide by the same principles that are established for the European Union Member States.[95] Moreover, the Directive makes it illegal for companies to transfer personal information to other companies unless they too, subscribe to the Directive.[96] Unfortunately, the standards applied to privacy rights by the United States fall short of the Directive.[97] The Directive, for example, applies stricter rules on the regulation of information used in marketing.[98] A data subject must be explicitly informed of the transfer of his or her personal data and must be given the chance to object to such transfers of information.[99] Moreover, sensitive information such as an individual's racial and ethnic background, political affiliation, religious or philosophical beliefs, trade-union membership, sexual preferences, and health are not allowed to be collected at all unless

93. Anna Shimanek, Note, *Do You Want Milk With Those Cookies?: Complying with Safe Harbor Privacy Principles*, 26 IOWA J. CORP. L. 455, 462-463 (2001).

94. Council Directive 95/46 art. 1, 1995 O.J. (L 281) 31 (EU).

95. The Institute IEEE, *Countries Strengthen Privacy Laws*, Apr. 1, 2001, http://www.theinstitute.ieee.org/portal/site/tionline/menuitem.130a3558587d56e8fb2275875bac26c8/index.jsp?&pName=institute_level1_article&TheCat=2202&article=tionline/legacy/INST2001/apr01/fprivacy.xml& (last visited Apr. 26, 2009).

96. *Id.*

97. Sullivan, *supra* note 31.

98. Privacilla, *The EU Data Privacy Directive*, http://www.privacilla.org/business/eudirective.html (last visited Apr. 26, 2009).

99. *Id.*

the individual consents to the collection of the sensitive information.[100]

These regulations have become an inconvenience for many American businesses, requiring them to spend additional dollars so that they can comply with the principles of the Directive when doing business abroad.[101] In fact, when the Directive was first implemented, e-commerce between the United States and Europe almost came to a halt. In order to facilitate the continued transfer of personal information for business purposes, the United States and the European Union had to come to an agreement that would streamline the privacy objectives of both entities.[102] In 2000, the European Commission and the U.S. Department of Commerce created the "safe harbor" framework.[103] The safe harbor framework provides a cost efficient alternative to meeting the main principles of the Directive.

In order to become a member of the safe harbor and therefore, be considered to comply "adequately"[104] with the privacy protection standards of the European Union, an organization must first publicly declare that it intends to comply with the seven requirements of the safe harbor agreement. The organization must then self-certify with the Department of Commerce in writing each year by stating that it agrees to abide by the safe harbor requirements and publish a statement indicating that its privacy policy adheres to those requirements.[105] The seven requirements of the safe harbor are similar to those recommended by the OECD: (1) Notice—individuals must be notified of the purpose for which information is being collected about them and must have contact information on the organization that is collecting the information, (2) Choice—individuals must have the option to opt out of having their personal information be disclosed to a third party or used for purposes other than the original reason for collection, (3) Onward transfers (transfer to third parties)—organization must apply notice and choice standards to transfer information to a third party and the third party must subscribe to the safe harbor principles or an equivalent level of privacy

100. *Id.*
101. *Id.*
102. Sullivan, *supra* note 31.
103. Safe Harbor Overview, *supra* note 33.
104. *Id.*
105. *Id.*

protection, (4) Access—individuals must have access to personal information in order to correct, amend, or delete information, (5) Security—organizations must take reasonable precautions to protect information, (6) Data Integrity—information collected must be relevant for purposes of its use, and (7) Enforcement—recourse mechanisms must be in place to ensure compliance.[106] Once an organization joins the safe harbor, it will be considered "adequate" and data flow to the company will be free of restrictions.[107] Moreover, any claims that are brought by citizens of the European countries will be heard in the United States.[108]

2. Regulation of Investigatory Powers Act of 2000

The Regulation of Investigatory Powers Act of 2000 (RIPA) was not in force during the relevant time when *Copland* was decided. Today, however, it is a UK law that regulates the interception of communications. The adoption of RIPA was a reaction to the quick pace of technological advancements that allowed people and organizations to easily intercept both electronic and paper communications.[109] The provisions of the law make it illegal to intentionally intercept "any communication" without the authority to do so. RIPA is limited in that it only applies to interceptions that are conducted through a public postal service or a public telecommunication system.[110] Several grounds must be satisfied before any surveillance can be authorized. The surveillance must be: (a) in the interests of national security, (b) for the purpose of preventing or detecting crime or of preventing disorder, (c) in the interests of the economic well-being of the United Kingdom, (d) in the interests of public safety, (e) for the purpose of protecting public health, (f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department, or (g) for any purpose not falling within (a) through (f) which is specified by an order made by the Secretary of State.[111]

---

106. *Id.*
107. *Id.*
108. *Id.* ("subject to limited exceptions").
109. Regulation of Investigatory Powers Act, 2000, c.23 (Eng.) [hereinafter RIPA].
110. *Id.*
111. Ibrahim Hasan, *RIPA and Employee Surveillance*, INFORMATION LAW TRAINING, Apr. 2007, at 1, *available at* http://www.informationlaw.org.uk.

In the case of *Copland*, RIPA may have affected the Court's analysis regarding the interception of the Ms. Copland's telephone calls. The case, however, does not specifically describe what the College did to intercept or gather information from Ms. Copland's calls. According to RIPA, an interception of a telecommunication system involves: (a) a modification or interference with the system or its operation, (b) monitoring transmissions made by means of the system, or (c) monitoring of transmissions made by wireless telegraphy to or from an apparatus comprised in the system. [112] The main issue in *Copland* would have most likely been whether the College had the authority to intercept Ms. Copland's phone calls. To decide this issue, the Court would have probably balanced Ms. Copland's essential right to privacy with the College's justification for their actions and would have found that the College did not have the authority to intercept Ms. Copland's telephone calls. The College's justification would not have fallen within the specific grounds required by RIPA to conduct surveillance. Furthermore, a recent decision by the Investigatory Powers Tribunal seems to suggest that RIPA's broad definition of directed surveillance does not cover activities including surveillance of employees and service providers. [113] In *C v. The Police and the Secretary of State for the Home Department*, a former policeman argued that the police failed to get a RIPA authorization to do a directed surveillance on him. The Tribunal, however, found that RIPA did not apply to the police officer because, "[t]here is no real reason why the performance of the ordinary functions of a public authority should fall within the RIPA regime, which is concerned with the regulation of certain investigatory powers, not with the regulation of employees or of suppliers and service providers." [114]

The more controversial section of RIPA is Part III of the Act, which provides law enforcement additional powers to require people to disclose the "key" to any encrypted data that is being investigated. [115] A request to disclose the key to encrypted data must be approved by a judicial authority, chief of police, the

112. RIPA, *supra* note 109.

113. Hasan, *supra* note 111; C v. The Police and the Secretary of the State for the Home Department, Investigatory Powers Trib. No. IPT/03/32H (2006) [hereinafter C v. Home Department].

114. C v. Home Department, *supra* note 113 ¶ 85.

115. Jeremy Kirk, *Contested UK Encryption Discloser Law Takes Effect*, THE WASH. POST, Oct. 1, 2007, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/10/01/AR2007100100511.html.

customs and excise commissioner, or a person ranking higher than a brigadier or equivalent.[116] The section creates serious questions as to possible abuse or mishandling by the government but has yet to be fully challenged.[117]

In the business sector, Part III of RIPA will specifically create some difficulties regarding any information that is sent via a Blackberry. E-mails, for example, that are sent to a Blackberry are decrypted on the device itself, meaning that neither the manufacturer nor the wireless operator handling data transferred to a Blackberry has access to the encryption keys.[118] An investigator, therefore, would have to go directly to the device owner in order to obtain the "key." Part III of RIPA is also limited in that it only applies to data or information that is *stored* in the United Kingdom. Consequently any encrypted data that is simply transferred through the United Kingdom would not fall under the provisions of the Act.[119]

3. Employment Privacy Laws in Specific European Countries

Several Member States have also enacted their own privacy laws specifically directed at regulating employer practices for monitoring and surveying its employees.

i. Finland

In 2004, Finland enacted the Act on the Protection of Privacy in Working Life. The Act determines the legality of the collection and use of psychological genetic information, drug tests, medical histories, and video or audio surveillance in the workplace.[120] In November 2006, the Finnish Data Ombudsmann further explained that the Act barred employers from conducting internet searches on prospective employees unless consent was given by the prospective employee.[121]

---

116. *Id.*
117. *Id.*
118. *Id.*
119. *Id.*
120. Privacy International, *Privacy and Human Rights 2006: Country Report, Republic of Finland*, Dec. 18, 2007, *available at* http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559538.
121. *Id.*

ii. France

The Data Protection Act, amended in 2004, regulates the processing of personal information by government agencies and private entities.[122] Under the Act, any processing of personal data for medical research or by a public body must be done after registration and permission is given by the data protection authority, Commission Nationale de l'Informatique et des Libertés (CNIL).[123]

iii. Germany

Currently, Germany has no workplace privacy laws that regulate the use of employee personal data in the context of monitoring employee computer systems or web surfing.[124] Despite this, Germany has one of the strictest data protection laws in the European Union.[125] Recently, in 2001, the Federal Data Protection Act was amended to adjust the threshold number of employees needed within a company to require a data protection officer from four to nine. Consequently, many small companies, who were once obligated to have a privacy officer, are no longer required by statute to have one.[126]

iv. Italy

The Supervisory Authority for Personal Data Protection, Garante, enforces the Italian Data Protection Code.[127] In 2004, the Garante created guidelines for the use of video surveillance in schools, hospitals, on board transportation means, and in the workplace.[128] In addition, the Workers Charter prohibits employers from investigating the political, religious, or trade union

122. Privacy International, *Privacy and Human Rights 2006: Country Report, French Republic*, Dec. 18, 2007, *available at* http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559537.

123. *Id.*

124. Privacy International, *Privacy and Human Rights 2006: Country Report, Federal Republic of Germany*, Dec. 18, 2007, *available at* http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559535#[3].

125. *Id.*

126. *Id.*

127. Privacy International, *Privacy and Human Rights 2006: Country Report, Italian Republic*, Dec. 18, 2007, *available at* http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559525.

128. *Id.*

opinions of its employees, or on any matter that is unrelated to assessing the professional skills or aptitudes of its employees. [129]

v. Spain

In Spain, legislation is continually being presented to protect employee privacy rights. Currently, trade unions have been lobbying to deem employee e-mails as private communications, which would not be available to employers for viewing or tracking purposes. [130]

vi. Sweden

Legislation proposed in 2002 asked that employers be barred from having access to any "documented" personal data about employees. This would mean that employers could not even view any written notes on loose pieces of paper. The legislation also proposed to bar employers from viewing or tracking e-mails without the employee's consent, even if the employer has a policy of prohibiting its employees from using computer facilities for personal use. Additionally, under the legislation, employers would not be able to consider the criminal records of a candidate to make employment decision unless it is necessary for security reasons. [131]

vii. United Kingdom

The United Kingdom has drafted a "final code of practice" as a guideline for employers when handling personal information about its employees. Compliance with the code is optional but if a company neglects to comply with the guidelines, it will be under strict scrutiny of the Commissioner. The guidelines ban employers from monitoring staff communications and relying on automated processing of personal data to make hiring decisions. The guidelines also place the burden on the employer to justify its collection and storage of personal data. [132]

---

129. *Id.*

130. *Privacy Worldwide: Employee Privacy Heating Up Europe*, WILEY REIN LLP NEWSLETTER, Mar. 2002, http://www.wileyrein.com/publication_newsletters.cfm?ID=10&year=2002&publication_ID=10915&keyword= (last visited Apr. 26, 2009) [hereinafter *Privacy Worldwide*].

131. *Sweden Concerns Over Employer Monitoring*, 2 BNA WORLD DATA PROTECTION REP; *Privacy Worldwide*, *supra* note 130.

132. Cedric Laurant, *Privacy and Human Rights 2003: United Kingdom and Northern Ireland*, *available at* http://www.privacyinternational.org/survey/phr2003/countries/unitedkingdom.htm (last visited Apr. 26, 2009); *Privacy Worldwide*, *supra* note 130.

V. THE IMPLICATIONS ON U.S. TRANSNATIONAL CORPORATIONS

Before discussing how the disparities between United States' privacy laws and the privacy laws of Member States will affect U.S. transnational corporations, it is important to discuss whether Article 8 of the Convention even applies to private entities. Traditionally, the Convention has been applied only to public entities, but over time, it seems that the trend has changed. *Copland* clearly dealt with a public entity working on behalf of the State. In the future, however, it seems that globalization will force the Convention to take on a broader scope encompassing the conduct of private as well as public entities.

A. Do International Human Rights Obligations Apply to Private Entities?

1. Globalization

International human rights obligations were primarily aimed to protect individuals and groups from abusive action by States and State agents, however, globalization, marked by increased trade liberalization, privatization, and economic deregulation, has led to an emergence of powerful non-State actors with the capacity to violate human rights in ways that were not contemplated during the development of modern human rights.[133] As a result of globalization, some States have felt compelled to ease labor standards, modify tax regulations, and relax other standards to attract foreign investment, but this has only opened the door to further human rights violations.[134] The rise in information and communications technology, in particular, has threatened the right to the respect for private life.[135] Furthermore, a study done by the UN Economic and Social Council (UNESCO) has indicated that commerce in cultural property tripled between 1980 and 1991 under the impulses of satellite communications, internet, and videocassettes.[136] This development in globalization has posed challenges to international human rights law, because the law was

133. Symposium, *Globalization and the Erosion of Sovereignty in Honor of Professor Litchenstein: Protecting Human Rights in a Globalized World*, 25 B.C. INT'L & COMP. L. REV. 273, 273 (2009) [hereinafter Symposium, *Globalization*].

134. *See* Deborah Spar & David Yoffie, *Multinational Enterprises and the Prospects for Justice*, 52 J. INT'L AFF. 557, 557 (1999).

135. Symposium, *Globalization*, *supra* note 133, at 297.

136. *Id.* at 297.

not originally designed to regulate the conduct of non-State actors or to allow intervention in weak States when human rights violations occur.[137]

According to Dinah Shelton, Professor of Law at Notre Dame Law School, "Globalization today is most often associated with economic interdependence, deregulation, and a dominance of the marketplace that includes a shifting of responsibilities from State to non-State actors."[138] Eventually, the principal threat to human rights will be posed by multinational corporations, multilateral intergovernmental organizations, and transnational criminal syndicates or organized terrorists.[139] This threat has led to an increased concern about the responsibilities of all international actors to ensure the promotion and protection of human rights.[140] In fact; the UN Development Program devoted its *2000 Human Development Report* to "Human Development and Human Rights" where it specifically stated, "global corporations can have enormous impact on human rights—in their employment practices, in their environmental impact, in their support for corrupt regimes or in their advocacy for policy changes."[141] The report further stated that "rights make human beings better economic actors" and placed emphasis on the need for judicial reform to ensure the respect of human rights by private entities.[142]

Imposing human rights obligations on private entities is further supported by the language of basic human rights documents such as the Universal Declaration of Human Rights (Universal Declaration)[143] and the American Declaration of the Rights and Duties of Man (American Declaration).[144] Although these declarations are not binding, they've become instrumental in setting guidelines for every State's human rights laws. The Universal Declaration refers to itself as "a common standard of achievement for all people and all nations, to the end that every

137. *Id.* at 279.
138. *Id.* at 276-77.
139. *Id.* at 293.
140. *Id.* at 301.
141. U.N. Development Programme, *Human Development Report 2000*, at 1 (2000), *available at* http://hdr.undp.org/en/media/hdr_2000_ch0.pdf.
142. *Id.*
143. Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. GAOR, 3d Sess., at 71, U.N. Doc. A/810 (1948) [hereinafter Universal Declaration].
144. American Declaration of the Rights and Duties of Man, Ninth International Conference of American States, O.A.S. Res. XXX, art. XXIX, O.A.S. Off. Rec. OEA/ser. L./V/I.4 Rev. (1965) [hereinafter American Declaration].

individual, and every organ of society" shall strive to promote respect for, and observance of, the rights.[145] Article 30 of the Universal Declaration also states that, "nothing in this Declaration may be interpreted as implying for any state, group or person any right to engage in any activity or to perform any act aimed at the destruction of any of the rights and freedoms set forth herein."[146] Similarly, the American Declaration begins its preamble with encouragement to *all individuals* to conduct themselves with respect for the rights and freedoms of others.[147] From this, it can be inferred that the principle of respecting human rights applies to all societal relations, locally, regionally, and globally by State or non-State actors.[148]

As a result of the increased attention to the responsibilities of private entities under international law, international organizations have begun to directly regulate the behavior of non-State actors.[149] The Sub-Commission on the Promotion and Protection of Human Rights[150] and the United Nations Commission on Human Rights, for example, have both adopted resolutions on globalization and human rights.[151] The Working Group established by the Sub-Commission for the Prevention of Discrimination and Protection of Minorities has begun to evaluate how existing human rights standards apply to transnational corporations, including private initiatives and codes of conduct, and has also begun to collect for study, international, regional, and bilateral investment agreements.[152] The UN Global Compact has also received more than 1,500 company signatures, asking

145. Universal Declaration, *supra* note 143.

146. *Id.* at art. 1.

147. American Declaration, *supra* note 144 (emphasis added).

148. Symposium, *Globalization*, *supra* note 133, at 284.

149. *Id.* at 301.

150. The Sub Commission is the main subsidiary body of the Commission on Human Rights. It was established by the Commission in 1947 under the authority of the Economic and Social Council. Sub-Commission on the Promotion and Protection of Human Rights, http://www.unhchr.ch/html/menu2/2/sc.htm.

151. *See* U.N. ESCOR, 51st Sess., 58th mtg., U.N. Doc. E/CN.4/Res/1999/59 (1999); U.N. ESCOR, 52d Sess., 32d mtg., U.N. Doc. E/CN.4/Sub.2/Res/2000/7/ (2000).

152. *See* The Relationship Between the Enjoyment of Economic, Social and Cultural Rights and the Right to Development, and the Working Methods and Activities of Transnational Corporations, Sub-Commission on Prevention of Discrimination and Protection of Minorities Res. 1998/8, U.N. ESCOR, 50th Ses., 26th mtg., U.N. Doc. E/CN.4/Sub.2/Res/1998/8 (1998).

participants to support nine principles in the areas of human rights, labor, and the environment.[153]

Beyond the direct responsibilities of non-State actors, States themselves now have the increased burden of monitoring and controlling the actions of private entities to ensure that human rights violations do not occur within their jurisdiction.[154] The Trail Smelter Arbitration, Corfu Channel Case, and the UN Survey of International Law seem to further assert that both home and host States have an obligation to regulate the conduct of multinational companies.[155] Additionally, States can be held responsible for the failure to exercise diligence in controlling the behavior of non-State actors such as transnational corporations.[156] These extra duties and responsibilities placed upon both State and non-State actors, however burdensome they may be, ensure that globalization may continue to prosper. They protect the right to property, including intellectual property, freedom of expression and communication across boundaries, due process for contractual or other business disputes, and a remedy before an independent tribunal when rights are violated.[157] Without the protection of these rights, globalization would cease to exist.

2. Application of Article 8 to Private Entities

Although Article 8 of the Convention originally applied only to public entities, the "new climate of human rights" has given private employers cause to also provide privacy rights to its employees under the Convention.[158] In fact, the Council of Europe's Parliamentary Assembly has recognized that Article 8 "should not only protect an individual against interference by public authorities, but also against interference by private persons, or institutions, including the mass media."[159] It would be inconsistent to assume that privacy violations can only occur

153. SustainAbility Ltd., *The Changing Landscape of Liability, A Directors Guide to Trends in Corporate Environmental, Social and Economic Liability*, at 10-16, 27-30 (2004), *available at* http://www.sustainability.com/publications/Liability/The%20Changing-Landscape-of-Liability%202004.pdf [hereinafter *The Changing Landscape of Liability*].

154. Symposium, *Globalization*, *supra* note 133, at 301.

155. *See* Trail Smelter Arbitration, 3 U.N. R.I.A.A. 1905 (1931-41); Corfu Channel Case, 1949 I.C.J. 22 (1949).

156. Symposium, *Globalization*, *supra* note 133, at 305.

157. *Id.* at 285.

158. *See* Ward, *supra* note 83.

159. Resolution on the Protection of Privacy, *supra* note 67.

through public entities. "[B]ugging devices are, for example, available not only to the 'organs of the State' but also to private individuals. A 'tap' by the police and a 'bug' by a private detective result in equivalent violations of rights as far as the victim is concerned."[160] The main question, therefore, is whether the Member States have a positive obligation to protect its people from not only the invasions of privacy by public entities but also the actions of private entities within the State.

In *Airey v. Ireland* and *X and Y v. The Netherlands* the ECHR suggests that States do have a positive obligation with regard to Article 8 of the Convention.[161] In both cases, the State violated Article 8 by not providing adequate protection for the victims within the legal system. The court, however, was sure to explain that the State would not be held responsible to pay compensation for every private attack on a victim, but that State responsibility would arise when it has failed to secure the rights of the Convention to everyone within its jurisdiction.[162] Section 1 of Article 8's reference to "public," has therefore been interpreted to have legal force against both public and private actors.[163] Moreover, these results are justified on the basis that in reality, it is virtually impossible to separate the private sphere from the public sphere. Attempting to do so would create complicated legal problems of drawing lines and creating definitions of what is public and what is private in an environment that has tended to blend and mix the two spheres.[164] With respect to private corporate actors, Clapham, author of *Human Rights Obligations of Non-State Actors*, argues:

> [T]here is no evidence that the international legal order cannot accommodate duties for other kinds of actors. Although there are only rare instances where a corporation could be the respondent in a dispute before an international tribunal, a non-State actor such as a corporation can still be the bearer of international duties outside the context of international courts and tribunals. Lack of international jurisdiction to try a corporation does not mean that the corporation is under no

160. ANDREW CLAPHAM, HUMAN RIGHTS OBLIGATIONS OF NON-STATE ACTORS 214 (2006) [hereinafter CLAPHAM, NON-STATE ACTORS].

161. *See* Airey v. Ireland, 32 Eur. Ct. H.R. (ser. A) (1985); X and Y v. The Netherlands, 91 Eur. Ct. H.R. (Ser. A) (1985).

162. CLAPHAM, NON-STATE ACTORS, *supra* note 160, at 215.

163. *Id.* at 214.

164. CLAPHAM, PRIVATE SPHERE, *supra* note 63, at 93.

> international legal obligations. Nor does it mean that we are somehow precluded from speaking about corporations breaking international law.[165]

The implications of this interpretation is unclear, however, two major consequences will follow: (1) at the international level, States will become obligated to prevent individuals from having their privacy interfered with in a system that is both practical and effective and (2) at the national level, Article 8 will now be available as a tool to directly attack private bodies in national courts where the Convention has domestic status.[166]

B. How will Private Entities be Impacted by the Disparity in Privacy Interpretations?

1. Increased Risk of Litigation

The failure to reconcile the differences between privacy laws of the United States and other Member States will most likely increase the risk of litigation both domestically and internationally. The difficulty of enforcing guidelines established by the Universal Declaration and the American Declaration is that the guidelines are legally non-binding. Human rights lawyers, therefore, have turned to litigation as a tool for change and concrete interpretations of the law.[167] Consumers, workers, local communities, nongovernmental organizations (NGOs), and investors have all gone to the courts in hopes of remedying human rights violations.[168] Although most cases are unsuccessful, corporations have been found defending themselves in front of judges more frequently than ever before.[169] The shift to global free markets and instant communication also means that corporate activities can be scrutinized more closely and widely than ever.[170]

Despite a low success rate, it seems that the trend is moving towards more accountability being placed on corporations for their transnational actions. The old strategies used by corporations to avoid litigation are slowly being weakened. Courts, especially in cases involving human rights violations, have placed less emphasis

---

165. CLAPHAM, NON-STATE ACTORS, *supra* note 160, at 31.
166. CLAPHAM, PRIVATE SPHERE, *supra* note 63, at 212.
167. *The Changing Landscape of Liability*, supra note 153, at 27.
168. *Id.* at 10.
169. *Id.*
170. *Id.* at 16.

on the defense of *forum non conveniens* and specifically in the United States and the United Kingdom, the courts have rejected traditional arguments of sovereignty.[171] The courts have also become more welcoming of foreign plaintiffs. In 2000, the UK House of Lords opened the English courts to foreigners who had been injured overseas as a consequence of the operations of British companies or their subsidiaries.[172] In the United States, the Alien Tort Claims Act (ATCA) has also resurfaced as a viable option for plaintiffs to sue corporations. ATCA states, "district courts shall have original jurisdiction of any civil action by an alien for a tort only, committed in violation of the law of nations or a treaty of the United States."[173] And in 2003, the Ninth Circuit heard a major case under ACTA where it found that a company could be challenged in court simply for knowingly assisting human rights violations in the supply chain.[174] This increased risk of litigation has gone so far that some corporations have made the ultimate decision to end their international business investments. A survey by the Ashridge Center for Business and Society found that due to certain human rights issues, more than one in three of the five hundred largest companies have abandoned proposed investment projects and nearly one in five have divested their operations in a different country.[175]

2. Effect of *Copland's* Expanded Privacy Rights

The decision in *Copland v. United Kingdom* reflects the broad scope with which the ECHR is willing to interpret Article 8 of the Convention. Without specifically addressing domestic law, the court came to its conclusion based solely on the language of Article 8 of the Convention. This suggests that at the very least, U.S. businesses operating in States that are party to the Convention will no longer be able to collect information on their employees regarding telephone, e-mail, and internet usage. The information obtained by Carmarthenshire College was minimal according to U.S. standards. The College only collected information that was automatically generated from the telephone calls, e-mails sent, and internet websites visited. Such information

171. *Id.* at 11, 15.
172. *Id.* at 29.
173. *Id.* at 27.
174. *Id.* at 15.
175. *Id.* at 317.

included telephone numbers dialed, dates and times of the phone calls, length of the phone calls, a list of websites visited, times and dates of the visits, duration of each website visit, a list of e-mail addresses used, and the dates and times the e-mails were sent. In the United States, employers have broad rights to review not only the sort of information that was obtained by Carmarthenshire College, but also to review the contents of the communications facilitated by phone calls, e-mails, and internet usage.[176]

The effect *Copland* may have is also great considering the number of organizations that monitor their employees through one method or another. Generally, larger companies are more likely to engage in monitoring activity. The same can probably be said for the companies that tend to do business abroad in Europe. As U.S. corporations realize that they can no longer sustain their capacities or profits by merely conducting all of their business operations within U.S. borders, the natural tendency is to look elsewhere around the globe for business and profits. And as other countries continue to develop their services and stretch their reach to its customers, the oceans will seem less significant.

Although Americans believe that their privacy rights are heavily protected, they would be surprised to see how much more heavily European countries have protected the privacy of their citizens, especially against business corporations. Unlike the United States, European countries are more afraid of the invasion of privacy rights by private businesses rather than the government. For the most part, in Europe, the government is exempt from the majority of privacy right protections provided to individuals.[177]

Not only must U.S. businesses face restrictions established by Article 8 of the Convention, but they must also abide by the restrictions that are "in accordance with the law."[178] These privacy laws vary from country to country but most are even more protective than Article 8, such as the Directive discussed above.[179] The Directive requires all Member States to adopt laws that coincide with the terms of the Directive.[180] Consequently, U.S.

176. Sullivan, *supra* note 31.

177. *Id.*

178. The Convention, *supra* note 16.

179. *See* Council Directive 2008/58, 2002 O.J. (L 201) 37 (EC).

180. *Id. See also* Europa: European Countries, http://www.europa.eu/abc/european_countries/index_en.htm (last visited Apr. 26, 2009) (The European Union currently has twenty-seven member states: Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany,

corporations which choose to conduct business abroad in Europe must comply with not only Article 8 of the Convention, but also the Directive, and the specific laws which have been established or adopted by each individual European country.[181]

U.S. corporations must, therefore, make a judgment call on whether to expand their business operations across the seas in hopes of increasing their presence in a globalizing market, at the cost of perhaps decreased productivity or control over resources due to minimal surveillance capabilities. It becomes a balance of interests. On the one hand, there are many benefits to monitoring employee activities, both from a production and a legal standpoint. As far as productivity and efficiency in the workplace, employers have often used monitoring devices to prevent shirking and their actions seem to be justified. In one study, the results indicated that employees use the internet 75.5 percent of the time for their work while 24.5 percent of their time is dedicated to personal agendas such as reading the news, viewing pornography, day trading, or keeping up on sports scores.[182] Another study published in 1999 found that one in three workers surf the internet for personal interests during their work hours.[183] The lack of privacy in the workplace is further justified on the grounds that employment is conditioned on employees using employer premises to achieve employer goals and objectives, not personal objectives.[184] Employers have also found that electronic monitoring of employees provides more concrete and accurate data that can be consolidated and recorded so that problem areas can be more easily identified or resolved.[185] Monitoring has also been considered a useful procedure for evaluating employee performance, which is used for making promotion decisions or

---

Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom. The European Member States are also subject to the Convention).

181. Evans, *supra* note 32, at 1137 ("Academics have posited that there are certain 'first principles' that delineate internationally shared norms about data use and privacy in general. These principles express concern about the quality of data, transparency in the processing of data, the extra care warranted by sensitive personal data, and how standards should be enforced. How these basics are interpreted and incorporated into national legal systems may be a function of societal and cultural characteristics of nations.").

182. Regina Lynn Preciado, *Mouses to the Grindstone*, WIRED NEWS, Aug. 12, 1998, http://www.wired.com/news/culture/0,1284,14371,00.html (last visited Apr. 26, 2009).

183. Evans, *supra* note 32, at 1116.

184. Fazekas, *supra* note 52.

185. *Id.*

decisions on specific areas of training that need to be emphasized.[186]

From a legal perspective, employee surveillance is compelling because it acts as a measure to deter or capture employees who may commit tortious acts. Employers have a strong interest in preventing employees from inappropriate or unprofessional behavior such as employee theft, disclosure of confidential or proprietary information, and sexual harassment.[187] Moreover, employers generally have the duty to ensure a safe working environment and the safety of those who will foreseeably come into contact with their employees.[188] Accordingly, the computer is a powerful instrument that can be used by an employer to prevent situations where it may be found vicariously liable for certain unlawful acts. Interestingly, failing to monitor their employees sufficiently may also pose problems for corporations in suits involving negligent retention. Under negligent retention, an employer may be found liable for an employee's acts if the employer "should have known" of the employee's unlawful acts. Consequently, if monitoring employee activity is a common and cost efficient method of supervision, the failure to implement monitoring devices could be used against the employer.[189]

On the other hand, U.S. corporations must weigh the decreased abilities to monitor employees against the benefits of expanding operations abroad. While going abroad may increase a corporation's presence in the marketplace and increase profits from reduced overhead labor costs, the profits will not be as great if the employer is unable to ensure that acceptable work is actually being completed. Other questions arise from choosing to expand overseas. For example, how should the corporation align its business practices in its home State with its offices in other States? What sort of procedures should be put into place to account for employees that constantly travel between States? How easily can monitoring devices be turned on and off? How will the corporation account for changes or different interpretations in privacy laws that will affect how the business is run? How much

186. Frank J. Cavico, *Invasion of Privacy in the Private Employment Sector: Tortious and Ethical Aspects*, 30 HOUS. L. REV. 1263, 1299 (1993).

187. *Id.* at 1287.

188. N. PETER LAREAU, LABOR AND EMPLOYMENT LAW § 270.03[4], 270.18-270.19 (2004).

189. Fazekas, *supra* note 52.

does the corporation value control over its resources and employees compared to the value of competing with the forces of globalization?

Alternatively, transnational corporations that have already opened their offices in other States face the question of whether it is beneficial to maintain operations in a particular State by complying with local privacy laws. In fact, Google Inc., owner of the well-known internet search engine that reaches every corner of the earth, has come across this exact situation.[190] In 2006, the corporation chose to fight a U.S. subpoena for its user data in a lawsuit by Viacom Inc. for copyright infringement.[191] Despite Google's attempt to protect its users' personal data, it has faced much scrutiny from the European Union. After a year long investigation, the EU's Article 29 Data Protection Working Party informed Google that it must reduce the amount of time it stores user information in order to comply with EU privacy laws.[192] As a result, Google cut its storage time to eighteen months.[193] Google has made sacrifices in order to maintain its operations in Europe, but doing so hasn't put the corporation in the clear yet. "Google faces potential fines, private damages claims, and most importantly, reputational harm if users' personal data are shared with Viacom in violation of EU data privacy rules.... The mere fact that a U.S. court has ordered the transfer would not provide an adequate legal basis for disclosing European users' personal data."[194] Google is, therefore, stuck in a situation where it must determine whether it should comply with U.S. orders or EU orders.

The decision in *Copland* is perhaps just one of many to come that will interpret human rights obligations differently than the United States; in which case, transnational corporations, such as Google, must constantly monitor the activities of the courts and legislative bodies to ensure there are no violations of international human rights laws.

---

190. Stephanie Bodoni, *Google May Face New Round of Privacy Complaints*, THE BOSTON GLOBE, July 5, 2008, at A8-9.

191. *Id.* at A8.

192. *Id.* at A9.

193. *Id.*

194. *Id.* (quoting Wim Nauwelaerts, lawyer in the Brussels office of Hogan & Hartson LLP).

VI. REMEDIES

While there are currently no specific methods of determining how a U.S. corporation should approach the prospect of opening offices in other countries,[195] there are certain guidelines and principles they can follow to ensure they have the information needed to make an informed decision. Transnational corporations that are already abroad should make a thorough assessment of the political conditions and human rights practices in each country they are present by:

- Assessing the business for current or potential exposure to human rights risks;
- Making sure the company's business principles, codes of conduct, and internal policies are up to date on human rights;
- Comparing human rights standards for consistency in all operations globally;
- If involved in areas requiring abnormal levels of security by public or private forces at the site of a project, ensuring contracts with security include a requirement to respect human rights;
- Knowing which voluntary principles or standards the company is committed to and continunally check for compliance to the letter and spirit of these principles;
- Building internal education at all levels of management to new norms and expectations of corporate behavior in relation to human rights.[196]

In order to reduce the risk of violating different forms of legislation and ensure compliance with the majority of

---

195. *The Changing Landscape of Liability*, *supra* note 153, at 13, 15 (In 2000, a Corporate Code of Conduct Bill was introduced to the U.S. Congress which proposed a code of conduct for U.S.-based corporations with more than twenty employees abroad. The Code covered labor rights, human rights, transparency and environmental protection, and enlisted detailed provisions for enforcement, but unfortunately, the bill did not pass. The International Right to Know Coalition in the United States is currently promoting legislation that would require U.S. companies to report on key environmental, human rights, and labor issues.). *Id.* at 27 (In 2000, the U.S. and UK governments drafted an initiative called the Voluntary Principles on Security and Human Rights. This initiative calls for improved risk assessment when businesses contract with local governments, and for human rights protection to be written into contracts with security forces.). *Id.* (Recently, the UN established a set of Norms on the Responsibility of Transnational Corporations and Other Business Enterprises for human rights and they carry the weight of a formal UN authorized consultative process.).

196. *Id.* at 30.

requirements common to European States regarding privacy, it is recommended that U.S. employers:

- Provide notice to employees in a published policy on personal data the business collects, the uses of these data and why these uses are important to the business.
- Note in the policy whether monitoring will occur and what privileges, if any, an employee has to access internet and telephone facilities for personal use. State the reasons why monitoring of employees is necessary (e.g., productivity, security, protection of the firm from liability, legal requirements to assist law enforcement, etc.) Member States, however, may restrict employee monitoring even if a privacy policy reserves the right to monitor and forbids personal use of communication facilities.
- Determine whether employees' representatives or trade unions have a right of consultation in the development of the privacy policy. In addition, businesses should consider whether negotiations with employees' representatives concerning privacy would be beneficial. A negotiated result could ameliorate perceptions of privacy invasions, which could adversely affect employee morale, retention and recruitment, as well as a company's image.
- Enforce your privacy policy, as some Data Protection Authorities (DPAs) have stated that companies' actual practices, not their formal policies, are controlling.
- Determine whether Member State law requires your business to register databases of employee information.
- Obtain employees' verifiable consent to personal data handling, in particular for: (a) processing of "sensitive data" (e.g., personal information concerning health, ethnicity, and trade union status); (b) personal data transfers from or disclosures to third parties; (c) direct marketing; and (d) transfers of personal data outside of Europe. Nonetheless, EU DPAs may challenge the validity of an employee's consent if the circumstances appear coercive. And in certain cases, employee consent will be per se invalid.

- Provide employees a reasonable opportunity to access personal information stored about them and to correct errors they can show to exist.
- Develop mechanisms for updating employee information and checking for accuracy.
- Ensure that files and databases containing personal information are secure and handled only by personnel trained in your company's security policy.
- Examine the various methods for transferring personal data to nations outside of Europe in compliance with the Directive, such as joining the Safe Harbor program or entering into privacy contracts. [197]

VII. CONCLUSION

Depending on how a business interprets the ECHR's analysis in *Copland,* the decision either creates more limitations on how far an employer can go to monitor its employees, or it creates an even more abstract line separating the needs of a corporation with the private interests of individuals. The ECHR significantly expanded the scope of Article 8 of the Convention to include all correspondence in the workplace. This expansion of privacy rights raises several issues of concern for private organizations that have recently been subject to the human rights obligations originally only seen as a concern for public entities. Globalization has enabled private entities to diversify their markets, but at the same time, certain considerations must be made with regard to international interpretations of law that affect international business practices.

The privacy perspectives held in the United States compared to those held in Europe, for example, are markedly different. These differences require private entities to create separate business policies and procedures for its employees depending on where they are located. The mere location of an employee will change how a corporation chooses to monitor or store a particular employee's personal information. Moreover, complications will arise when an employee is needed to travel between locations or when information must cross a large body of water. Consequently, a transnational business must weigh its production and performance interests against its human rights obligations.

---

197. *Privacy Worldwide, supra* note 130.

After *Copland*, many questions still remain. Will the broad scope of Article 8 of the Convention cause businesses to enact more innovative methods of tracking performance or efficiency levels of their employees? Will there be other interpretations of the European privacy laws? How does the Convention provide for abuses or mishandling of information? And is it really possible or even practical for an employer to comply with all of the privacy restrictions set in place to protect employees? These same questions apply to the scope of human rights obligations in general and, ultimately, corporations will have to choose between the interests of sovereignty and the benefits of globalization.

Frances Ma[*]

[*] J.D. Candidate, May 2009, Loyola Law School, Los Angeles, California.