Employer Monitoring of Employee Electronic Mail and Internet Use

Charles Morgan*

The issue of e-mail and internet monitoring has received a great deal of attention, both in the media and in legal writing, especially in the United States. Moreover, with increasing frequency, employers and employees alike are seeking answers to two seemingly simple, inter-related questions: may employers legally monitor employee e-mail and Internet use? If so, under what circumstances?

Canadian courts have yet to address these questions head on. On the basis of a handful of American decisions, several Canadian commentators have responded to these questions more or less unequivocally: employers *may* monitor under any circumstances they deem fit. The responses seem to be based on two premises, both taken from American jurisprudence on the subject. First, employees have no reasonable expectation of privacy when using company e-mail and Internet facilities. Second, since the employer owns these work tools, he can monitor their use in any way deemed fit.

This article challenges both these premises and this form of analysis. It is currently impossible to provide a single, easy answer to the two questions as posed since the countervailing rights of employers and employees will vary in Canada, depending on a number of factors. Furthermore, it would be imprudent to nssume that Canadian courts will follow American jurisprudence on the subject of e-mail and Internet use monitoring, since significant differences exist between applicable American and Canadian privacy legislation.

Privacy principles gleaned from *Charter* jurisprudence, judicial interpretation of privacy legislation, and pending legislation suggest that employees have a reasonable expectation of privacy in their use of e-mail and the Internet in the workplace setting and that employers have a right to monitor such use only if the monitoring is performed reasonably and in accordance with employees' consent or on the basis of a compelling specific interest.

Le problème de la surveillance du courrier électronique et de l'internet a été l'objet de beaucoup d'attention dans les médias et dans la doctrine juridique, surtout aux États-Unis. Les employeurs et employés sont de plus en plus fréquemment à la recherche de réponses à deux questions reliées et apparemment simples : les employeurs peuvent-ils légalement surveiller l'utilisation par leurs employés du courrier électronique et de l'internet ? Si oui, dans quelles circonstances ?

Les tribunaux canadiens n'ont toujours pas répondu directement à ces deux questions. En se fondant sur une petite quantité de décisions américaines, plusieurs commentateurs canadiens ont répondu à ces questions plus ou moins sans équivoque : les employeurs *peuvent* surveiller dans toute circonstance qui leur semble appropriée. Ces réponses semblent fondées sur deux prémisses empruntées de la jurisprudence américaine sur le sujet. Premièrement, les employés ne peuvent s'attendre raisonnablement à la protection de leur vie privée lorsqu'ils se servent du courrier électronique et de l'internet de la compagnie. Deuxièmement, comme l'employeur est propriétaire de ces outils, il peut surveiller leur utilisation dans toute manière appropriée.

Cet article défie ces deux prémisses et cette forme d'analyse. Il est actuellement impossible de fournir une seule réponse facile à ees deux questions puisque les droits des employeurs et employés varient à travers le Canada selon une variété de facteurs. De plus, il serait imprudent de présumer que les tribunaux canadiens suivront la jurisprudence américaine à ce sujet puisqu'il existe des différences importantes entre les législations américaine et canadienne applicables.

Les principes de la vie privée, dérivés de la jurisprudence sur la *Charte*, de l'interprétation judiciaire des lois sur la vie privée et même des lois qui ne sont pas encore en vigueur, suggèrent que les employés puissent s'attendre raisonnablement à la protection de leur vie privée lorsqu'ils se servent du courrier électronique ou de l'internet en milieu du travail. Les employeurs ont le droit de surveiller cette utilisation seulement si la surveillance est conduite de façon raisonnable et si l'employeur respecte le consentement des employés ou se base sur un intérêt particulier convaincant.

* B.A. (Toronto), Maîtrise (Paris IV-Sorbonne), B.C.L., LL.B. (McGill). The author practices technology and communications law at McCarthy Tétrault, Montreal. The author wishes to thank Yan Paquette and David Roberge of McCarthy Tétrault for their invaluable research assistance.

To be cited as: (1999) 44 McGill L.J. 849
Mode de référence : (1999) 44 R.D. McGill 849

Introduction

Use of electronic mail ("e-mail") and the Internet has become an integral part of the workplace. A recent survey by International Data Corp. (Canada) Ltd., a computer consulting company, found that 50% of all Canadian households include at least one person with regular access to the Internet, up from 37% in January 1998 and 31% in April 1997. Of the 40.4% of Canadian adults with Internet access, 56% are connected at work.[1]

E-mail and the Internet offer a vast array of benefits to corporations, such as improved communication among employees, improved customer support, efficient research capacity, and new means of establishing "brand" presence in a potentially global context. Nevertheless, many employers are concerned about the down-side of easy access to the Internet and e-mail by their employees. Many employers are concerned, for instance, that employees waste time "browsing", rather than using the Internet efficiently and productively. Moreover, employers are concerned that employees might obtain access to or post illegal materials over the Internet—such as child pornography or copyright-protected documents—or that employees might make defamatory statements via e-mail or the Internet for which employers could be liable. Finally, some are concerned that employees might transmit important trade secrets over the Internet either deliberately or inadvertently. In short, employers want to protect their investment in high technology, ensure that their employees are working productively, and avoid any liability that might result from inappropriate use of the corporate computer network.

For these reasons, many employers have begun monitoring employee use of e-mail and the Internet. An American Management Association ("AMA") survey conducted in 1998 indicates that two-thirds of surveyed organizations practice one or more forms or electronic monitoring.[2] More specifically, 43% monitor employees from time to time via video or audio taping and/or via the storage and review of computer files (including e-mail). This latter figure is up from 35% found in the 1997 AMA survey. The survey did not provide specific figures for the monitoring of Internet use, but one may derive a rough estimate of such monitoring from the 20.2% of employers who indicated that they stored and reviewed e-mail messages (up from 19.76% in 1997).

---

[1] Intemational Data Corp. (Canada) Ltd., "The Canadian Consumer Internet Market: Second Quarter Report, May-June 1999" *The Globe and Mail* (10 May 1999) B1.

[2] American Management Association, *1998 AMA Survey: Workplace Testing and Monitoring*, online: American Management Association <http://www.amanet.org/research/pdfs/WT&M=2c_a.pdf> (date accessed: 26 October 1999).

Unsurprisingly, the issue of e-mail and Internet monitoring has received a great deal of attention both in the media[3] and in legal writing,[4] especially in the United States. Moreover, with increasing frequency employers and employees alike are seeking answers to two seemingly simple, interrelated questions. First, may employers monitor employee e-mail and Internet use? Second, if so, under what circumstances?

Canadian courts have yet to address these questions head-on. On the basis of a handful of American decisions, several Canadian commentators have responded to these questions more or less unequivocally: (i) yes; and (ii) as the employer sees fit. The response seems to be based on two premises, both taken from American jurisprudence on the subject. First, employees have no reasonable expectation of privacy when using company e-mail and Internet facilities. Second, since the employer owns these work tools, he can monitor their use in any way he deems fit.

This article challenges both these premises and this form of analysis. It presents the following arguments:

(1) It is currently impossible to provide a single, easy answer to the two questions as posed since the countervailing rights of employers and employees will vary in Canada depending, among other things, on whether the employee works in the public or private sector; whether the employee works in

---

[3] See *e.g.* T. Johnston, "Quit watching me!" *The Globe and Mail* (29 January 1999), online: The Globe and Mail <http://www.globeandmail.com> (date accessed: 29 January 1999); M. Evans, "Your boss is watching" *The Globe and Mail* (17 September 1998), online: The Globe and Mail <http://www.globeandmail.com> (date accessed: 17 september 1998); D. Shepherd, "E-mail Security: Becoming Big Brother," Quicken <http://www.quicken.ca/eng/soho/online-office/email/index.html> (last modified: 20 November 1998); and H.L. Rasky, "Can an employer search the contents of its employees' e-mail?" (1998) 20 Advocates' Q. 221. For American discussion, see M. Goldstein & L. Vogel, "Can you read your employees' e-mail?" *New York Law Journal* (24 February 1997), online: New York Law Journal <http://www.nylj.com> (date accessed: 24 February 1997); and J.F. Lomax Jr., "Privacy in the Workplace" *South Carolina Lawyer Magazine* (January-February 1998) 14, online: South Carolina Bar <http://www.scbar.org/scbar/reference/sclawyer/1998jf-a1.stm> (date accessed: 2 August 1998).

[4] See *e.g.* D. Johnston, S. Handa & C. Morgan, *Cyberlaw: What You Need to Know About Doing Business Online* (Toronto: Stoddart, 1997) at 66ff.; M.S. Dichter & M.S. Burkhardt, "Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age" (American Employment Law Counsel Fourth Annual Conference, Grove Park Inn, Asheville, North Carolina, 2-5 October 1996), online: Morgan, Lewis & Bockius LLP <http://www.mlb.com/speech1.htm#Seminars> (date accessed: 26 October 1999); A.L. Lehman, "E-mail in the Workplace: Question of Privacy, Property or Principle" (1997) 5 Com. L. Conspectus 99; J. White, "e-mail@work.com: Employer Monitoring of Employee E-mail" (1997) 48 Ala. L. Rev. 1079; R. Fitzpatrick, "Technology Advances in the Information Age: Effects on Workplace Privacy Issues" in American Law Institute & American Bar Association, *ALI-ABA Course of Study: Current Developments in Employment Law* (Washington: American Law Institute & American Bar Association, 1997) 599; and R.M. Schall, "Employee Privacy Rights" in Practicing Law Institute, *Wrongful Termination Claims: What Plaintiffs and Defendants Have to Know* (Washington: Practicing Law Institute, 1998) 865.

Quebec or in a common law province; whether, in the latter case, the province has enacted specific privacy protection legislation or relies on the common law; whether the employee is subject to a collective bargaining agreement or to an individual employment contract; and whether the employer has contractually established a right of monitoring by means of a monitoring policy, or otherwise.

(2) It would be imprudent to assume that Canadian courts will follow American jurisprudence on the subject of e-mail and Internet use monitoring, since significant differences exist between applicable American and Canadian privacy legislation.

(3) The judicial and legislative trend in Canada is toward ever greater protection of individual privacy rights, particularly in the last five years.

(4) Privacy principles gleaned from jurisprudence arising out of the *Canadian Charter of Rights and Freedoms*,[5] judicial interpretation of privacy legislation, and pending legislation suggest that employees have a reasonable expectation of privacy in their use of e-mail and the Internet in the workplace and that employers have a right to monitor such use only if the monitoring is performed reasonably and in accordance with employees' consent or on the basis of a compelling specific interest.

(5) Privacy rights and property rights are not mutually exclusive: the fact that an employer owns the computer equipment used by employees does not, *per se*, provide an unfettered right to monitor use.

Given the element of high technology involved in questions concerning e-mail and the Internet, it is perhaps tempting to consider the phenomenon of employer e-mail and Internet surveillance in isolation, as a technology law issue only. Such an approach would be imprudent. The issue of employer monitoring of employee e-mail and Internet use takes one to the confluence of several distinct but related areas of law—privacy, employment, surveillance, and high technology—sometimes referred to as "cyberlaw". Accordingly, this article treats each of these areas of law and implicitly poses the questions: what is new about employer monitoring of e-mail and Internet use as opposed to other forms of electronic surveillance? What is not?[6]

The article begins by examining the nature and scope of the right of privacy. It then poses the question as to why privacy rights have become such a significant legal and social issue relatively recently. The article then presents an overview of the legislative privacy framework in the United States and Canada, which are compared and contrasted. Next, the article examines both the competing and converging interests of employers and employees with respect to the monitoring of employee e-mail and

---

[5] Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11 [hereinafter Canadian *Charter*].

[6] See also Johnston, Handa & Morgan, *supra* note 4 at c. 1.

Internet use. Finally, the article explores recent jurisprudence with respect to electronic surveillance in the workplace, in both the collective bargaining context and that of the individual contract of employment.

I. What is Privacy?

While it is beyond the scope of this article to establish the precise nature and scope of the right of privacy,[7] it is nonetheless important to canvass some of the more significant doctrine and judicial findings on the subject so as to understand more fully the right to which many employees lay claim.

Territorial privacy, as traditionally understood in English common law, was directly linked to the notion of personal property. In *Semayne's Case*,[8] the House of Lords held that "the house of every man is to him as his castle and fortress, as well for his defence against injury and violence, as for his repose," and hence to enter it uninvited constituted trespass. Similarly, in *Entick* v. *Carrington*,[9] Lord Camden held that "our law holds the property of every man so sacred, that no man can set his foot upon his neighbour's close without his leave: if he does he is a trespasser, though he does no damage at all."

English common law protected the individual against bodily intrusions by means of an action in assault: any non-consensual bodily contact by a third party constitutes assault at common law.

Finally, the common law protected one's personal papers and matters from public exposure via copyright and/or the charge of defamation.

A. A Personality Right

These three notions—territorial or spatial privacy, personal privacy, and informational privacy—have come to be notionally distinguished from the concept of ownership over time. Rather than finding their basis in property rights, doctrinal writers, courts, and legislators in the United States and Canada have all come to hold that the right of privacy is a "personality right". The very nature of a personality right is that it is held by everyone and that it cannot be alienated. It is extra-patrimonial. It is in part for this reason that it is inappropriate to suggest that ownership rights negate privacy rights. The two kinds of rights are each of a different nature; they overlap, they are not mutually exclusive.

When Samuel Warren and Louis Brandeis set out to draft the seminal "The Right to Privacy," published in the Harvard Law Review in 1890, their stated purpose was to

---

[7] For a more complete review of the question, see P. Burns, "The Law and Privacy: The Canadian Experience" (1976) 54 Can. Bar Rev. 1.

[8] (1604), 77 E.R. 194, [1588-1774] All E.R. Rep. 62 at 91b (H.L.).

[9] (1765), 95 E.R. 807, 2 Wils. K.B. 275 (H.L.).

determine whether the existing law held a principle by which individuals could protect their privacy from the prying eyes of the media, specifically tabloid press. After reviewing existing case law, they came to the conclusion that "the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the more general right of the individual to be let alone."[10] Moreover, they found that the principle upon which this right rests is not the principle of private property, but rather that of "inviolate personality."[11] Warren and Brandeis write:

> [T]he rights, so protected, whatever their exact nature, are not rights arising from contract or special trust, but are rights against the world; and ... the principle which has been applied to protect these rights is in reality not the principle of private property ... [but rather] the right of privacy.[12]

From jurisprudence which invoked this acknowledged personality right—the right to be let alone—William Prosser in an article published in the California Law Review in 1960 found four distinguishable common law torts: (i) intrusion into one's private affairs; (ii) public disclosure of private facts; (iii) appropriation of one's personality; and (iv) publicity that place one in a false light in the public eye.[13] Certain authors attempted to identify an underlying commonality to these torts;[14] others, such as Paul Freund, suggested that such efforts at categorization only served to impoverish the abstract legal principle.[15]

B. Privacy: Grounded in the Concept of Physical and Moral Autonomy

In Canada, some of the most principled language on the nature, scope, and importance of privacy stems from a series of decisions of the Supreme Court.[16] Since the

---

[10] S. Warren & L. Brandeis, "The Right to Privacy" (1890-91) 4 Harv. L. Rev. 193 at 205.

[11] Warren & Brandeis, *ibid.* at 205.

[12] *Ibid.* at 213.

[13] W.L. Prosser, "Privacy" (1960) 48 Cal. L. Rev. 383. Prosser's enumeration of invasion of privacy torts provided the basis for the American *Restatement (Second) of the Law of Torts* § 652A(2) (1967). See further F. Allard, "La vie privée : cet obscur objet de la prestation contractuelle" in Centre de recherche en droit privé et comparé du Québec, Université McGill, *Mélanges Paul-André Crépeau* (Cowansville, Qc.: Yvon Blais, 1997) 9.

[14] See R.B. Parker, "A Definition of Privacy" (1973-74) 27 Rutgers L. Rev. 275.

[15] P. Freund, "Privacy: One Concept or Many" in J.R. Pennock & J.W. Chapman, eds., *Privacy: NOMOS XIII* (New York: Atherton Press, 1971) 182. Note also A.F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967) at 31, 32 where the author discusses four "states" of privacy: solitude, intimacy, anonymity, and reserve. H.P. Glenn, for his part, speaks of two "rights": the right of solitude which protects one against intrusion and the right of anonymity which protects one against exposure: see H.P. Glenn, "Le droit au respect de la vie privée" (1979) 39 R. du B. 879.

[16] A second source of doctrine on privacy stems from commentary on the Quebec *Charter of Human Rights and Freedoms*, R.S.Q. c. C-12 [hereinafter Quebec *Charter*], which pre-dates the Canadian *Charter*. Quebec has the strongest privacy legislation in Canada: see *e.g.* Glenn, *ibid.*, perhaps the leading article in Quebec doctrine on the subject of privacy.

introduction of the Canadian *Charter* in Canada in 1982, a growing body of Supreme Court jurisprudence has treated a particular embodiment of the general right of privacy, namely, the right against unreasonable search and seizure set forth in section 8.[17]

In *Hunter* v. *Southam Inc.*,[18] the Supreme Court of Canada held that one of the main purposes of section 8 was "to protect individuals from unjustified state intrusions upon their privacy."[19] In *R.* v. *Dyment*,[20] the Supreme Court explored the issue of privacy in greater detail. The case involved a doctor who had taken a blood sample from an emergency patient for medical purposes while the patient was unconscious. The blood sample was then given to the police when it was found that it provided evidence of impaired driving. The majority of the Supreme Court held that this constituted an unreasonable search and seizure. It found that the taking of a blood sample involves one of the most serious violations of personal privacy: it infringes upon the individual directly. The fact that the sample was taken for justifiable medical purposes did not justify its use for non-medical purposes. In order to obtain the blood sample legitimately, the police should have obtained either a warrant or the patient's consent.

Writing for the majority and concurring with Dickson J.'s findings in *Hunter*, La Forest J. discussed the notion of privacy at length. Citing Alan Westin[21] with approval, he noted that privacy is at the heart of liberty in a modern state. La Forest J. writes:

> Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order. The restraints imposed on the government to pry into the lives of the citizen go to the essence of a democratic state.[22]

C. Territorial, Personal, and Informational Privacy

Adopting a framework of analysis originally put forth in *Privacy and Computers*,[23] La Forest J. describes three zones of privacy to which courts should be espe-

---

[17] The Quebec *Charter* is discussed below. As shall be seen, s. 5, which states that "[e]very person has a right to respect for his private life," initially had very little impact on Quebec privacy protection jurisprudence. This phenomenon appears to be in the process of changing.

[18] [1984] 2 S.C.R. 145, 11 D.L.R. (4th) 641 [hereinafter *Hunter* cited to S.C.R.].

[19] *Ibid.* at 160. Dickson J. did not limit the purpose of s. 8 to privacy protection, but rather found that, at very least, it protected the privacy interest. He states: "I would be wary of foreclosing the possibility that the right to be secure against unreasonable search and seizure might protect interests beyond the right of privacy, but for purposes of the present appeal, I am satisfied that its protections go at least that far" (*ibid.* at 159).

[20] [1988] 2 S.C.R. 417, 55 D.L.R. (4th) 503 [hereinafter *Dyment* cited to S.C.R.].

[21] *Supra* note 15 at 349-50.

[22] *Dyment, supra* note 20 at 427-28.

[23] *Report of the Task Force established by the Department of Communications & the Department of Justice: Privacy and Computers* (Ottawa: Communication Group, 1972) at 12-14 [hereinafter *Privacy and Computers*].

cially alert: territorial, personal, and informational. He describes each of these zones at length:

> Territorial claims were originally legally and conceptually tied to property, which meant that legal claims to privacy were largely confined to the home. But as Westin ... has observed "[t]o protect privacy only in the home ... is to shelter what has become, in modern society, only a small part of the individual's daily environmental need for privacy."[24]

With respect to privacy of the person, a right invoked in situations such as a direct physical search of the person or the taking of a blood sample for purposes of drug testing or otherwise, La Forest J. concurred with Lamer J.'s highlighting the particular seriousness of violating the sanctity of a person's body.[25] Moreover, La Forest J. cites *Privacy and Computers*: "Our persons are protected not so much against the physical search (the law gives physical protection in other ways) as against the indignity of the search, its invasion of the person in a moral sense."[26]

Finally, La Forest J. discusses informational privacy:[27]

> In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the person to whom, and restricted to the purposes for which it is divulged, must be protected.[28]

The Supreme Court decision in *Dyment* highlights two privacy principles that have been stated and restated in documents as varied as the OECD Guidelines on Privacy Protection, the CSA Model Privacy Code, and the recent federal Bill C-54: namely "consent" and "limited use". That is, in general, people legitimately expect that personal information will only be used with their consent and for the purposes for which it was collected.

D. Privacy and Context

We do not always expect that our acts and deeds will remain private. The scope of the private realm varies depending on the person, the location, the epoch, and the culture in question. As Westin has noted, it also varies greatly depending on the governing political system: a characteristic of totalitarianism is that it virtually annihilates

---

[24] *Dyment, supra* note 20 at 428.

[25] See *R.* v. *Pohoretsky*, [1987] 1 S.C.R. 945, 39 D.L.R. (4th) 699.

[26] *Supra* note 23 at 13.

[27] In *R.* v. *Duarte*, [1990] 1 S.C.R. 30 at 46, 74 C.R. (3d) 281 [hereinafter *Duarte* cited to S.C.R.], La Forest J. focuses on informational privacy and suggests that privacy may be defined as "the right of the individual to determine for himself when, how, and to what extent he will release personal information about himself."

[28] *Dyment, supra* note 20 at 429-30.

the private realm; a characteristic of democracy is that it promotes a broad private sphere.[29]

Pierre Trudel suggests that there are both objective and subjective determinants of the scope of privacy.[30] Certain physical locations, such as the home, are given special status as an "objectively" private realm. Similarly, certain personal objects, such as diaries, toiletries, or even one's blood are so privileged. Finally, information regarding such personal matters as sexual orientation or state of health are deemed to be particularly worthy of privacy protection. At the same time, any and all of these factors may be affected by subjective factors, Trudel suggests. One must ask whether, under the circumstances, the public (or certain members thereof) holds a legitimate right to be informed of matters stemming from this private sphere. Similarly, one must ask whether, under the circumstances, the individual holds a reasonable expectation of privacy.

In relation to section 8 of the Canadian *Charter*, the Supreme Court of Canada has, on a number of occasions, addressed the concept of an "expectation of privacy".[31] In *R.* v. *Plant*,[32] Sopinka J. delineated a framework for the determination of a person's "reasonable expectation of privacy" based on the analysis of a number of contextual factors:

> Consideration of such factors as the nature of the information itself, the nature of the relationship between the party releasing the information and the party claiming its confidentiality, the place where the information was obtained, the manner in which it was obtained and the seriousness of the crime being investigated allow for a balancing of the societal interests in protecting individual dignity, integrity and autonomy with effective law enforcement.[33]

E. Limits to the Right of Privacy

Thus, although fundamental, the right of privacy is not absolute. Warren and Brandeis held that the right of privacy must necessarily be limited, finding that among other things, the right did not prohibit publication of matter which is of public or general interest or for which the publisher has obtained consent.[34] Westin concurs:

> The functions of privacy in liberal systems do not require that it be an absolute right. The exercise of privacy may create dangers for a democracy that may call for social and legal responses. ... Thus the constant search in democracies must be for the proper boundary line in each specific situation and for an over-all equilibrium that serves to strengthen democratic institutions and processes.[35]

---

[29] *Supra* note 15 at 23.

[30] See generally P. Trudel, *Droit du Cyberespace* (Montreal: Thémis, 1997) at c. 11.

[31] See *e.g. Hunter*, *supra* note 18; and *Dyment*, *supra* note 20.

[32] [1993] 3 S.C.R. 281, 12 Alta. L.R. (3d) 305 [hereinafter *Plant* cited to S.C.R.].

[33] *Ibid.* at 293.

[34] *Supra* note 10 at 216, 218.

[35] *Supra* note 15 at 25.

La Forest J. echoes this sentiment in *Duarte*: "It thus becomes necessary to strike a reasonable balance between the right of individuals to be left alone and the right of the state to intrude on privacy in furtherance of its responsibilities for law enforcement."[36]

Where it comes into conflict with other societal needs, courts must undertake a balancing exercise between individual privacy rights and the countervailing rights of individuals, groups, or society at large. In law enforcement situations, for instance, Canadian courts have acknowledged the efficacy and legitimacy of surreptitious electronic surveillance so long as it is carried out in accordance with a valid prior authorized warrant.[37] In the case of journalistic and artistic endeavours, the Supreme Court has acknowledged the need to balance the right of privacy against freedom of expression.[38] In the case of employees, as we shall see, labour arbitrators and courts have long recognized the need for employers to protect against theft, vandalism, or other misconduct.

II. Why Now?

Although it would be inaccurate to suggest that assertions of the importance of privacy are new phenomena, it is likely that the issue has never before been of such central importance in the public mind. In a 1993 Ekos research survey, 92% of Canadians surveyed expressed concern about their personal privacy.[39] Why has privacy come to have such a significant place on the public and legal agenda? Three elements of a response are suggested here.

A. Technology

New technology makes it possible to intrude upon territorial, personal, and informational privacy as never before.[40] Several commentators have explored the increased relevance of privacy resulting from the onslaught of new information technology. Already in 1890, Warren and Brandeis attributed the need for privacy to "the intensity and complexity of life, attendant upon advancing civilization."[41] Freund argues that "the formation of a distinct concept of privacy ... reflected claims of democracy and pressures of technology."[42] Édith Deleury and Domenique Goubau similarly cite the

---

[36] *Supra* note 27 at 45.

[37] See *Duarte, ibid.* at 44.

[38] See *Edmonton Journal* v. *Alberta (A.G.)*, [1989] 2 S.C.R. 1326, 64 D.L.R. (4th) 577; and *Aubry* v. *Éditions Vice-Versa Inc.*, [1998] 1 S.C.R. 591, 157 D.L.R. (4th) 577 [hereinafter *Vice-Versa* cited to S.C.R.].

[39] Online: Ekos Research Associates <http://www.ekos.com> (date accessed: 29 November 1998).

[40] Ann Cavoukian and Don Tapscott chronicle many of the ways in which new technology has had the effect of eroding personal privacy in the workplace in *Who Knows: Safeguarding Your Personal Privacy in a Networked World* (Toronto: Random House, 1995) at 115-127. See also Johnston, Handa & Morgan, *supra* note 4 at 66-87.

[41] *Supra* note 10 at 196.

[42] *Supra* note 15 at 187.

development of new technology and the democratisation of modern society as two of several factors that make privacy rights "un trait de la civilisation contemporaine."[43]

In *Duarte*, the Supreme Court addressed the issue of privacy and electronic surveillance. The case involved a police investigation into drug trafficking. Police rented an apartment equipped with audio-visual recording equipment. Pursuant to section 178.11(2)(a) of the *Criminal Code*[44]—which excepts the interception of conversations to which one of the parties consents from the prohibition of unauthorized electronic surveillance—the police informer and undercover police officer consented to the interception of their conversations. The appellant discussed a cocaine transaction in the presence of the two others, which was recorded electronically without his consent. The Supreme Court had to determine whether surreptitious, electronic, participant surveillance without prior authorization from a competent authority constituted an unreasonable search and seizure. The Court found for the appellant; the surveillance was in breach of section 8 of the Canadian *Charter*. According to La Forest J.:

> [T]he regulation of electronic surveillance protects us ... not [from] the risk that someone will repeat our words but from the much more insidious danger inherent in allowing the state, in its unfettered discretion, to record and transmit our words. ... The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private.[45]

B. Democracy

As mentioned above, the privileging of privacy is intimately linked to a belief in the virtue of democracy. Alan Westin, in *Privacy and Freedom*, discusses the functions of privacy in democratic society. He identifies four specific functions: (i) the development of personal autonomy; (ii) the facilitation of emotional release; (iii) the opportunity for self-evaluation; and (iv) the encouragement of limited and protected communication. Of these, the first is particularly important for the development of healthy democracy. Westin writes:

> This development of individuality is particularly important in democratic societies, since qualities of independent thought, diversity of views, and nonconformity are considered desirable traits for individuals. Such independence requires time for sheltered experimentation and testing of ideas, for preparation

---

[43] É. Deleury & D. Goubau, *Le Droit des personnes physiques*, 2d ed. (Cowansville, Qc.: Yvon Blais, 1997) at 153-67.

[44] R.S.C. 1985, c. C-46.

[45] *Duarte*, *supra* note 27 at 44. La Forest J. also cites Douglas J., dissenting in *United States* v. *White*, 401 U.S. 745, 91 S. Ct. 1122 (1971) [hereinafter *White* cited to U.S.]: "Electronic surveillance is the greatest leveler of human privacy ever known."

> and practice in thought and conduct, without fear of ridicule or penalty, and for the opportunity to alter opinions before making them public.[46]

What is true of society as a whole is true of the workplace. If a workplace is to foster independence and creativity, privacy must be respected. Business processes adopted in the workplace are indicative of how employers perceive their employees:

> Corporations with elaborate modes of employee monitoring and control, for example, implicitly suggest that their employees are untrustworthy. Manifold levels of management, organized in a pyramidal, hierarchical structure, suggest that there are significant differences in human capacities; that our differences are more important than our similarities.[47]

While business practices modelled on nineteenth century industrialism and social Darwinism have been tenacious, they are also manifestly on the wane. In an information economy, so-called "Taylorist" business practices are counter-productive. Vast bureaucracies with elaborate mechanisms of monitoring and control lack the flexibility required to adapt to the current pace of technological change. Moreover, such bureaucracies under-exploit the collective knowledge of their employees by underestimating and under-stimulating them. Newer business practices, more in keeping with the principles of workplace democracy, place greater responsibility in the hands of employees and downplay the need for heavy surveillance. In such a context, the demands for the respect of personal privacy increase. Widespread efforts at monitoring employees by means of new technology thus seem strangely anachronistic.[48]

C. *The Canadian* Charter

Prior to the introduction of the Canadian *Charter* in Canada, privacy rights were afforded little weight. As will be discussed below, Canadian common law—following English rather than American common law—contained no general right of privacy. Moreover, while the federal government and a number of provinces enacted privacy legislation prior to the Canadian *Charter*, the statutes were rarely applied. Even in Quebec, where the right to the respect of one's private life had been enshrined in 1977 in the Quebec *Charter* at section 5, courts were reluctant to give the provision any real weight in the face of competing interests.

The Canadian *Charter* has dramatically changed the Canadian privacy landscape. Its characteristics as a constitutional document and as a promoter of individual rights have served to add bite to individual assertions of the privacy interest. As discussed

---

[46] *Supra* note 15 at 34. See also Westin, *ibid.* at 35, where his discussion of the need for "emotional release" is also illuminating. He argues that life in society generates such tensions for the individual that periods of privacy are necessary to ensure both physical and psychological health. Among other things, such private time acts as a safety valve, wherein individuals are able to vent anger at "the system" or "the boss" without fear of reprisal.

[47] Johnston, Handa & Morgan, *supra* note 4 at 41.

[48] See also M. O'Conner, "The Human Capital Era: Reconceptualizing Corporate Law to Facilitate Labor-Management Cooperation" (1993) 78 Cornell L. Rev. 899.

above, since 1982, the Supreme Court of Canada has explored the nature and scope of privacy protection afforded to individuals under section 8 of the Canadian *Charter* on several occasions. The relevance of such decisions to a private dispute between an employer and an employee, however, is subject to dispute. Section 32(1) of the Canadian *Charter* states:

> This Charter applies
>
> (a) to the Parliament and government of Canada in respect of all matters within the authority of Parliament including all matters relating to the Yukon and Northwest Territories; and
>
> (b) to the legislature and government of each province in respect of all matters within the authority of the legislature of each province.

On the basis of this provision, courts and commentators have generally asserted that the Canadian *Charter* only applies to government action and hence that it would have no application in a dispute between private parties which involves no act of government.[49] Nevertheless, a number of Supreme Court decisions have left room for an indirect impact of the Canadian *Charter* on private disputes.

In *Dolphin Delivery*, McIntyre J., writing for the majority, discussed the applicability of the Canadian *Charter* to private disputes.[50] He concluded that while the Canadian *Charter* does not apply to disputes between private parties, courts ought to apply and develop principles of common law in a manner consistent with the fundamental values enshrined in the Constitution. McIntyre J. writes:

> Where ... private party "A" sues private party "B" relying on the common law and where no act of government is relied upon to support the action, the *Charter* will not apply. I should make it clear, however, that this is distinct from the question whether the judiciary ought to apply and develop the principles of the common law in a manner consistent with the fundamental values enshrined in the Constitution. The answer to this question must be in the affirmative. In this sense, then, the *Charter* is far from irrelevant to private litigants whose disputes fall to be decided at common law.[51]

In *Dolphin Delivery*, McIntyre J., for a unanimous court, thus opened the possibility of applying "*Charter* values" to rules of common law in disputes involving private litigants. Although stated in *obiter*, the suggestion has been subsequently acted

---

[49] See *RWDSU* v. *Dolphin Delivery Ltd.*, [1986] 2 S.C.R. 573, 33 D.L.R. (4th) 174 [hereinafter *Dolphin Delivery* cited to S.C.R.]; *Tremblay* v. *Daigle*, [1989] 2 S.C.R. 530, 62 D.L.R. (4th) 634; *McKinney* v. *University of Guelph*, [1990] 3 S.C.R. 229, 76 D.L.R. (4th) 545; and P. Hogg, *Constitutional Law of Canada*, 4th ed. (Scarborough: Carswell, 1996) at 645ff. See *contra* D. Gibson, "The Charter of Rights and the Private Sector" (1982) 12 Man. L.J. 213; D. Gibson, "Distinguishing the Governors from the Governed: The Meaning of 'Government' under Section 32(1) of the Charter" (1983) 13 Man. L.J. 505; and M. Manning, *Rights, Freedoms and the Courts: A Practical Analysis of the Constitution Act, 1982* (Toronto: Emond Montgomery, 1983).

[50] *Ibid.* at 593ff.

[51] *Ibid.* at 603.

upon on several occasions. In *Dagenais* v. *Canadian Broadcasting Corp.*,[52] Lamer J., writing for the majority, cited McIntyre J. with approval, and concluded that it was necessary to reformulate the common law rule governing the issuance of publication bans in a manner that reflects the principles of the Canadian *Charter*. Lamer J. writes:

> The pre-*Charter* common law rule governing publication bans emphasized the right to a fair trial over the free expression interests of those affected by the ban. In my view, the balance this rule strikes is inconsistent with the principles of the *Charter*, and in particular, the equal status given by the *Charter* to ss. 2(b) and 11(d). It would be inappropriate for the courts to continue to apply a common law rule that automatically favoured the rights protected by s. 11(d) over those protected by s. 2(d). ... [T]he common law rule must be adapted so as to require a consideration both of the objectives of the publication ban, and the proportionality of the ban to its effect on protected *Charter* rights.[53]

In *Hill* v. *Church of Scientology of Toronto*,[54] Cory J., writing for the majority, highlighted the distinction between *Charter* rights and *Charter* values: "Private parties owe each other no constitutional duties and cannot found their cause of action upon a *Charter* right."[55] Nonetheless, in the context of civil litigation involving only private parties, the Canadian *Charter* will "apply" to the common law "to the extent that the common law is found to be inconsistent with *Charter* values."[56] Cory J. also suggested an approach for applying *Charter* values to the common law in circumstances involving private parties. He held that the balancing of competing values "must be more flexible than the traditional s. 1 analysis undertaken in cases involving government action. ... *Charter* values, framed in general terms, should be weighed against the principles which underlie the common law."[57] Finally, unlike typical *Charter* challenges, the party who is alleging that the common law is inconsistent with the Canadian *Charter* "should bear the onus of proving both that the common law fails to comply with *Charter* values and that, when these values are balanced, the common law should be modified."[58]

In *Hill*, Cory J. found that reputation, while not explicitly protected by the Canadian *Charter*, reflected the "innate dignity of the individual" and was "related to the right to privacy which has been accorded constitutional protection."[59] On this basis, he held that the common law of defamation should be amended so as to reflect *Charter* values more adequately. *A fortiori*, the common law of privacy protection has been

---

[52] [1994] 3 S.C.R. 835 at 878, 120 D.L.R. (4th) 12 [hereinafter cited to S.C.R.].

[53] *Ibid.* at 877-78. See also *R.* v. *Salituro*, [1991] 3 S.C.R. 654 at 675, 68 C.C.C. (3d) 289.

[54] [1995] 2 S.C.R. 1130, 126 D.L.R. (4th) 129 [hereinafter *Hill* cited to S.C.R.].

[55] *Ibid.* at 1170.

[56] *Ibid.* at 1171.

[57] *Ibid.*

[58] *Ibid.* See also *A.M.* v. *Ryan*, [1997] 1 S.C.R. 157 at 171-72, 143 D.L.R. (4th) 1; and Hogg, *supra* note 49 at 657ff.

[59] *Hill*, *ibid.* at 1179.

and will continue to be subject to amendments so as to render it in conformity with *Charter* values as expressed by the Supreme Court.

On the basis of these decisions, Peter Hogg concludes that the exclusion of the common law from *Charter* review is not particularly significant. "When the Charter does not apply directly, it will apply indirectly, and, despite some differences in the way s. 1 justification is assessed, the indirect application is much the same in its effect as the direct application."[60]

III. How Are Privacy Rights Protected Against Electronic Surveillance?

A. A Sketch of American Privacy Legislation and Jurisprudence

It is beyond the scope of this article to undertake a thorough comparative analysis of American and Canadian law on the subject of employer monitoring of employee e-mail and Internet use. American legislation, doctrine, and jurisprudence is cited extensively, but only to the extent that it has had an impact on Canadian law or may serve in its interpretation.

1. The Constitution of the United States

The right to privacy was placed on a constitutional footing in the United States in the case of *Katz* v. *United States*.[61] The Fourth Amendment of the Constitution of the United States provides:

---

[60] *Supra* note 49 at 662.

[61] 389 U.S. 347, 88 S. Ct. 507 (1967) [hereinafter *Katz* cited to U.S.]. *Katz* is cited in particular here because (i) it treats the notion of unreasonable search and seizure, (ii) it establishes privacy as a personality right rather than as a property right, and (iii) because it was cited with approval by the Supreme Court of Canada in *Hunter*, the first Supreme Court decision to recognize the constitutional right to privacy in Canada. *Katz*, however, was not the first or only source of constitutional protection of the right to privacy in the United States. In *Skinner* v. *Oklahoma*, 316 U.S. 535, 62 S. Ct. 1110 (1942), for instance, the United States Supreme Court struck down an Oklahoma state law which empowered the state to sterilize individuals convicted of multiple crimes involving "moral turpitude". The Supreme Court relied on U.S. Const. amend. XIV which bars Congress and State legislatures from depriving "any person of life, liberty or property ... without due process of law." In *Griswold* v. *Connecticut*, 381 U.S. 479, 85 S. Ct. 1678 (1965), the United States Supreme Court, on the basis of a "penumbra" of rights contained in the *Bill of Rights*—particularly in the First Amendment—struck down a Connecticut statute that prohibited the use of contraceptives by married couples. See also *Roe* v. *Wade*, 410 U.S. 113, 93 S. Ct. 705 (1973); *Loving* v. *Virginia*, 388 U.S. 1, 87 S. Ct. 1817 (1967); *Eisenstadt* v. *Baird*, 405 U.S. 438, 92 S. Ct. 1029 (1972); and *Roberts* v. *United States Jaycees*, 468 U.S. 609, 104 S. Ct. 3244 (1984). It is beyond the scope of this article to treat such cases of alternative constitutional bases for the right of privacy. Canadian constitutional protection of the right of privacy is found in the Canadian *Charter*, *supra* note 5, s. 8, which is analogous to U.S. Const. amend. XIV.

> The right of 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.

In *Katz*, Stewart J., delivering the majority opinion of the United States Supreme Court, held that "the Fourth Amendment protects people, not places."[62] Accordingly, the decision had the effect of rejecting any necessary link between the Fourth Amendment and the tort of trespass. Although Stewart J. did not identify the Fourth Amendment exclusively with the protection of the right of privacy, Dickson J., commenting on the case in the Supreme Court of Canada decision of *Hunter*, held that privacy protection "played a prominent role in [Stewart J.'s] construction of the nature and the limits of the American constitutional protection against unreasonable search and seizure."[63]

The Fourth Amendment of the Constitution of the United States protects individuals from unreasonable searches and seizures by federal authorities. This protection extends into the workplace of all federal and—through the Fourteenth Amendment—the states and State employers.[64] Only "unreasonable searches" performed where the employee has a "reasonable expectation of privacy" are unconstitutional. In the context of electronic communication monitoring, whether a search is unreasonable and the employee's privacy expectation is reasonable depends on several factors. These include the reason for the search or monitoring, whether the employer has a policy on point which would have diminished or eliminated the employee's privacy expectations, and the scope of the search. For private corporations which do not act as an agent of the State, jurisprudence relating to the Fourth Amendment is of little value and hence not discussed here.

2. The *Electronic Communications Privacy Act*

In 1968, the United States Congress adopted the *Federal Wire Tap Statute*.[65] The statute imposes criminal liability on the illegal use of technology to intercept and record telephone calls. In 1986, Congress amended the statute to extend the prohibition to the interception of electronic communications.[66]

Under Title 1, *ECPA* § 2511,[67] it is illegal for anyone to "intentionally intercept, endeavor to intercept, or procure any other person to intercept or to endeavor to intercept any ... electronic communication." The *ECPA* also prohibits the disclosure or use

---

[62] *Ibid.* at 351.

[63] *Supra* note 18 at 159.

[64] See *O'Connor* v. *Ortega*, 480 U.S. 709, 107 S. Ct. 1492 (1989) [hereinafter *O'Connor*].

[65] 18 U.S.C.A. § 2510 (West 1968).

[66] See *Electronic Communications Privacy Act of 1986*, Pub. L. No. 89-508 (1996) [hereinafter *ECPA*].

[67] *Ibid.*

of the contents of an electronic communication if the disclosing individual knows or has reason to know that the communication was intercepted.

Although nothing in *ECPA* § 2511 explicitly excludes the workplace from the scope of the Act, the language used in the provision, as well as the interpretation several American courts have given to it, have substantially limited its applicability to the monitoring by employers of employee use of e-mail and the Internet in the office environment. The Act defines "intercept" as "the aural or other acquisition of the contents of any ... electronic ... communication to the use of any electronic, mechanical, or other device."[68] According to *Steve Jackson Games Inc.* v. *United States Secret Service*[69] and *Wesley College* v. *Pitts*,[70] there can be no interception under Title 1 if the acquisition of the contents of electronic communication is not contemporaneous with their transmission. Because e-mail is often in transit for only a few seconds, and most often acquired only once it has been stored, Title 1 rarely applies to the monitoring of e-mail.

Moreover, there are two exceptions to the general rule against interception of electronic communications. First, *ECPA* § 2511(2)(d) provides that it is not unlawful to intercept the contents of an electronic communication when the intercepting party has obtained the consent of one of the parties to the communication. Such consent may be express—*e.g.* by having an employee sign a consent form relating to the monitoring of office e-mail—or implied—*e.g.* by the employee's use of the employer's e-mail system after the employee has been informed that employer monitoring actually takes place.[71] However, an employee's mere knowledge that the employer is capable of monitoring his communication may not be sufficient to provide consent in the absence of knowledge that the employer is actually monitoring.[72] Furthermore, there is no consent where the employer's monitoring activity exceeds the scope of its own policy. For example, a court will not find consent where the employer's policy states that it will monitor only the addresses to which and the frequency with which communications are sent, but, in actuality, the employer monitors the content of the messages as well.[73]

Second, the *ECPA* also provides a "business use exception" to the general prohibition of the interception of electronic communications. This exception applies where an officer, employee, or agent of a provider of wire or electronic wire or electronic communication services, "intercept[s], disclose[s], or use[s] that communication in

---

[68] *ECPA*, *ibid.*, § 2510(4).

[69] 36 F.3d 457 (5th Cir. 1994), online: LEXIS (GENFED/MEGA) [hereinafter *Steve Jackson Games*].

[70] 974 F. Supp. 375 (D. Del. 1997), online: LEXIS (GENFED/MEGA).

[71] See *Watkins* v. *L.M. Berry & Co.*, 704 F.2d 577 (11th Cir. 1993), online: LEXIS (GENFED/MEGA) [hereinafter *Watkins*].

[72] *Ibid.* at 581-82. See also *Deal* v. *Spear*, 980 F.2d 1153 (8th Cir. 1992), online: LEXIS (GENFED/MEGA).

[73] See *Watkins*, *supra* note 71.

the normal course of his employment while engaged in any activity which is necessarily incident to the rendition of his service or to the protection of the rights or property of the provider of that service."[74] Thus, where an employer is intercepting the e-mail of an employee, an exception to the general prohibition will apply where (i) the employer is the "provider" of the e-mail service, and (ii) the activity occurs in the normal course of the individual's employment. Courts often seem to take for granted that the employer is the provider of the e-mail system.[75] Most courts have concluded that any monitoring done by the employer is sufficiently related to its business interests as to fall within the exception.[76] On the other hand, where the employer is monitoring the content of personal e-mail—as opposed to merely monitoring to detect whether the e-mail is of a personal or business nature or monitoring the frequency with which personal e-mail is being sent—courts have held that the employer may not avail itself of the exception.[77]

Once an electronic communication has been transmitted and stored, temporarily or otherwise, it falls outside the purview of Title 1 of the *ECPA* and becomes subject to Title 2. The latter makes it unlawful to "intentionally access ... without authorization a facility through which an electronic communication service is provided" or to "intentionally exceed ... an authorization to access [a] facility."[78] Despite its potential application to employee e-mail-related privacy concerns, the storage provisions of the *ECPA* provide little protection for employees. This is because Title 2 provides a broad exemption for "the person or entity providing the wire or electronic communications service."[79] Thus, under the Act, an employer, assuming provider status, is free to access stored e-mail messages and other electronic communication irrespective of the nature (personal or professional) of the message and without regard to whether the employer has first received the employee's consent.[80]

3. American Common Law Privacy Torts

As discussed above, the American common law tort of invasion of privacy is an umbrella under which four different theories of liability reside: (i) placing a person in a false light, (ii) misappropriation of a person's name or image, (iii) publication of private facts, and (iv) unreasonable intrusion into the seclusion of another. If an employer does not disclose private information learned while monitoring employees, it will avoid liability under three of the four invasion of privacy theories.[81] By contrast,

---

[74] *ECPA*, *supra* note 66, § 2511(2)(a)(i).

[75] See *e.g. Bohach* v. *City of Reno*, 932 F. Supp. 1232 at 1236 (D. Nev. 1996), online: LEXIS (GENFED/MEGA) [hereinafter *Bohach*].

[76] See *Briggs* v. *American Air Filter Co.*, 630 F.2d 414 (5th Cir. 1980), online: LEXIS (GENFED/MEGA); and *Watkins*, *supra* note 71 at 582-85.

[77] *Watkins*, *ibid.*

[78] *ECPA*, *supra* note 66, § 2701(a).

[79] *ECPA*, *ibid.*, § 2701(c)(1): the "provider exception".

[80] See *Bohach*, *supra* note 75.

[81] See *Restatement (Second) of the Law of Torts* § 652A (1967).

an employee may prevail under the fourth theory of invasion of privacy if he shows that the employer's intrusion—by virtue of monitoring or surveillance—is highly objectionable to a reasonable person.[82]

The tort of unreasonable intrusion therefore has three elements: an "intrusion" which is "highly offensive" to a "reasonable person." As discussed by Dichter and Burkhardt,[83] American courts generally consider electronic surveillance—*e.g.* telephone monitoring—sufficient to establish the first element of the tort.[84] In order to determine the offensiveness of the intrusion, American courts have examined "the degree of intrusion, the context, conduct and circumstances surrounding the intrusion, as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded."[85] While express or implied consent is one defense to liability under this tort, the mere good faith belief that consent has been given is not normally a defense.[86]

With respect to the third element of the tort, American courts require both that the employee have a subjective expectation of privacy and that the expectation be objectively reasonable. American case law on this last point suggests that an employee will have little success in bringing a claim against an employer on the basis of this tort in the context of employer monitoring of employee e-mail.

In *Smyth* v. *Pillsbury Co.*,[87] the Pillsbury Corporation fired the plaintiff for making inappropriate comments on the company's e-mail system. The plaintiff then brought a wrongful discharge action, contending that Pillsbury had terminated him in violation of public policy, specifically his common law right to privacy. The court ultimately dismissed the plaintiff's cause of action, stating that he could not have reasonably expected his office e-mail messages to be private. The court so concluded even though Pillsbury supposedly had assured its employees that communication via e-mail would not be intercepted by management.[88] The court also held that even if the plaintiff had held a reasonable expectation of privacy, the employer would not be liable because "no reasonable person would consider the defendant's interception of [his] communications to be a substantial and highly offensive invasion of his privacy."[89]

---

[82] *Ibid.*, § 652B: "intrusion upon seclusion" is defined as "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of privacy, if the intrusion would be highly offensive to a reasonable person."

[83] *Supra* note 4.

[84] See *e.g. Billings* v. *Atkinson*, 489 S.W.2d 858, 16 Tex. Sup. Ct. J. 181 (1973); and *Nader* v. *General Motors Corp.*, 255 N.E.2d 765, 25 N.Y.2d 560 (N.Y. 1970).

[85] See *Miller* v. *National Broadcasting Co.*, 187 Cal. App. 3d 1463, 232 Cal. Rep. 668 at 679 (C.A. 1986).

[86] See *Crump* v. *Beckley Newspapers Inc.*, 320 S.E.2d 70, 173 W. Va. 699 (W. Va. 1983).

[87] 914 F. Supp. 97 (E.D. Pa. 1996), online: LEXIS (GENFED/MEGA) [hereinafter *Symth*].

[88] *Ibid.* at 100-01.

[89] *Ibid.* at 101.

The conclusions of the court in Pillsbury follow a trio of cases from California.[90] Two more recent cases, *United States* v. *Maxwell*[91] and *McVeigh* v. *Cohen*,[92] suggest that American courts acknowledge that e-mail users, especially those using a private service such as America Online, hold a reasonable expectation of privacy. Thus far, however, American courts have not extended the principle to the workplace.

4. *Smyth* v. *Pillsbury Co.*

Smyth merits a closer look because it has been so often cited as authority for the proposition that employees hold no reasonable expectation of privacy in the workplace context when using e-mail or the Internet. As mentioned above, in this case, the defendant company assured its employees that e-mail communications would not be intercepted or used against its employees as grounds for termination or reprimand.[93] In October 1994, the plaintiff received an e-mail message on his home computer sent by his supervisor using the company computer system. Relying on the defendant's assurances, the plaintiff responded in a manner deemed inappropriate and unprofessional. The company later obtained (the decision uses the word "intercepted") copies of these messages, and terminated the plaintiff's employment. The plaintiff brought forth a wrongful dismissal claim. The claim was rejected.

The court noted that Pennsylvania law does not provide a common law cause of action for the wrongful dismissal of an at-will employee such as the plaintiff, unless the discharge threatens or violates a clear mandate of public policy. After raising the possibility that the common law of Pennsylvania regarding tortious invasion of privacy might constitute a mandate of public policy, the court found that the plaintiff failed to state a claim upon which relief could be granted since he did not have a reasonable expectation of privacy in his e-mail communications with his supervisor.

Weiner J. of the Pennsylvania District Court held that he could not find "a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management."[94] He continues:

---

[90] See *Flanagan* v. *Epson*, Cal. Super. Ct., Los Angeles County, 1990, Docket No. B.C. 007036 (refusing to extend the right of privacy to e-mail); *Shoars* v. *Epson America*, Cal. Super. Ct., Los Angeles County, 1991, Docket No. S.W.C. 112749 (refusing to extend the right of privacy to e-mail); and *Bourke* v. *Nissan Motor Co.*, Cal. C.A., 26 July 1993, Docket No. B.O. 68705 (no reasonable expectation of privacy in one's e-mail).

[91] 45 M.J. 406 at 417-19 (U.S. Armed Forces C.A. 1996), online: LEXIS (GENFED/MEGA) [hereinafter *Maxwell*] (an individual has a reasonable expectation of privacy on e-mail sent via private service).

[92] 996 F. Supp. 59 (D.C. D. 1998), online: LEXIS (GENFED/MEGA).

[93] *Supra* note 87 at 98.

[94] *Ibid.* at 101.

> Once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost. ...
>
> [E]ven if we found that an employee had a reasonable expectation of privacy in the contents of his e-mail communications over the company e-mail system, we do not find that a reasonable person would consider the defendant's interception of these communications to be a substantial and highly offensive invasion of his privacy. ... [B]y intercepting such communications, the company is not, as in the case of urinalysis or personal property searches, requiring the employee to disclose any personal information about himself or invading the employee's person or personal effects. Moreover, the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments.[95]

Given the specific facts of the case, one should be wary of concluding that it stands for the general proposition that employees have no reasonable expectation of privacy when they use the company e-mail system. Smyth's e-mail was sent directly to his supervisor. No monitoring took place. The message was not really "intercepted" by the company (despite the wording of the judgment); the company, in a sense, was the intended recipient. The message was apparently retrieved from the supervisor's computer after he had received the message, as intended.

Moreover, the case is particular in that it involved an employee who apparently threatened violent action.[96] Under such circumstances, it is not surprising that the court concluded in *obiter* that the company's interest in preventing inappropriate "or even illegal" activity outweighed the plaintiff's privacy interests.

Furthermore, the court asserts that Smyth lost any reasonable expectation of privacy "once [he] communicated the alleged unprofessional comments to a second person ... over an e-mail system which was apparently utilized by the entire company."[97] As Anne Lehman points out, the logic of this argument is questionable, since it seems to suggest that the use of e-mail is like broadcasting, *i.e.*, a message is sent by one and is then available to all.[98] Typically, an e-mail message is sent point-to-point rather than point-to-multipoint. Although it may pass through several servers on its way from one point to the next, it is extremely rare that the message is intercepted or read *en route.*

Finally, one should note that the tort in question involves an intrusion which would be "highly offensive" to a reasonable person. There is no equivalent language in article 36 of the *Civil Code of Quebec*, the analogous provision related to breach of privacy, nor in Canadian statutory or common law privacy provisions.

---

[95] *Ibid.*

[96] The defendant alleged that the e-mails concerned sales management and contained threats to "kill the backstabbing bastards" and referred to a planned party as the "Jim Jones Koolaid affair."

[97] *Supra* note 87 at 101.

[98] *Supra* note 4.

B. An Overview of the Canadian Privacy Framework

Although it is tempting to simply apply the conclusions of American courts regarding the monitoring of employee e-mail and Internet use to the Canadian context, such an unqualified comparative analysis would be imprudent. As explored below, important differences exist between the relevant Canadian and American statutory language, suggesting that Canadian case law on the subject of employer monitoring of employee use of e-mail and the Internet will differ in its analysis and conclusions from the analysis and conclusions reached in the United States on the subject. There is no single "privacy law" that treats the issue of privacy protection in the Canadian workplace. The present section provides a sketch of the existing Canadian privacy legislative structure.[99]

1. International Accords

Canada is a signatory of a number of international agreements which protect personal privacy. The *Universal Declaration of Human Rights*,[100] proclaimed in 1948, was the first international instrument to recognize privacy as a human right. In the interim, Canada has become a signatory to such international instruments as the *International Covenant on Civil and Political Rights*[101] which also asserts the right of individuals to a respect for their privacy. Such instruments encourage governments to adopt privacy protection legislation, rather than protecting the privacy rights of individuals, in and of themselves.

In July 1995, the European Union formally adopted the *Directive on the Protection of Personal Data and the Free Movement of Such Data.*[102] The *Directive* prohibits the trans-border flow of personal information to countries without adequate privacy protection. In its draft form, the *Directive* had the effect of increasing pressure throughout North America to strengthen private sector data protection. In Canada, the *Directive* has been one of the factors that has led the federal government to bring Bill C-54[103] before the House of Commons. Bill C-54 sets forth rules governing the collection, handling, and dissemination of personal information in the private sector.

Moreover, Canada is a member of the International Telecommunications Union ("ITU"). As such, Canada must act in conformity with the privacy principles found in

---

[99] For a more complete review of privacy legislation in Canada see R. Laperrière & N. Kean, "Le droit des travailleurs au respect de leur vie privée" (1994) 35 C. de D. 709. See also Trudel, *supra* note 30.

[100] GA Res. 217(III), UN GAOR, 3d Sess., Supp. No. 13, UN Doc. A/810 (1948) 71, art. 12.

[101] (16 December 1966) 999 U.N.T.S. 171, 1976 Can. T.S. No. 47, art. 17.

[102] [1995] O.J. L. 2/281 [hereinafter the *Directive*].

[103] *Personal Information Protection and Electronic Documents Act*, 1st Sess., 36th Parl., 1997. Bill C-54 will be discussed in greater detail in Part III.*B*.3.*g*, below. Bill C-54 did not pass prior to the closing of the Parliamentary session, but it has gone through a third reading and has been passed by the House of Commons in substantially the same form as Bill C-6, *Personal Information Protection and Electronic Documents Act*, 2d Sess., 36th Parl., 1999.

article 37 of the ITU's constitution. To this end, it is of note that both the federal *Telecommunications Act*[104] and the *Radiocommunication Act*[105] contain privacy protection provisions.

2. Canadian *Charter* Privacy Protection

As discussed above, the right of privacy has attained constitutional protection by virtue of the Supreme Court's interpretation of section 8 of the Canadian *Charter* which protects individuals against unreasonable search and seizure. While the Canadian *Charter* does not extend constitutional privacy protection to individuals involved in private disputes—such as employers and employees acting in the private sector—*Charter* values have nonetheless had an indirect impact on the results of decisions by both courts and arbitrators treating disputes between employers and employees over electronic surveillance in the workplace, in the context both of collective agreements and individual employment contracts. This impact is discussed below.

In a 1997 decision, the Supreme Court of Canada explored a second constitutional source of privacy protection, namely the "right to liberty" under section 7 of the Canadian *Charter*. In *Godbout* v. *Longueuil (City of)*,[106] the Court had to determine whether a municipal resolution requiring all new permanent municipal employees to reside within its territorial limits breached section 7 of the Canadian *Charter* and/or section 5 of the Quebec *Charter*,[107] which guarantees "respect for [one's] private life." The minority held that the resolution breached both provisions. The majority, in two separate opinions, held that once it was determined that the resolution breached section 5 of the Quebec *Charter*, it was preferable to avoid pronouncing on the applicability of section 7 of the Canadian *Charter*.

3. Federal Privacy Legislation

The Canadian legislative framework with respect to privacy is complicated by the federal structure of its constitution which assigns the federal government jurisdiction over the matters listed in section 91 of the *Constitution Act, 1867*,[108] and which assigns the provincial governments legislative authority over matters listed in section 92. Perhaps unsurprisingly, "privacy" does not figure in either list, drafted as they were in 1867. Thus, while the federal government has enacted privacy legislation in respect of matters falling within its core competency such as criminal law, banks, telecommunications companies, and Canada Post, and while provincial governments have enacted privacy legislation by virtue of their jurisdiction over matters of property and civil rights, there is no single, overarching privacy regime.

---

[104] S.C. 1993, c. 38, ss. 7(i), 41.

[105] R.S.C. 1985, c. R-2, s. 9(1)(b).

[106] [1997] 3 S.C.R. 844, 152 D.L.R. (4th) 577 [hereinafter *Godbout* cited to S.C.R.].

[107] *Supra* note 16.

[108] (U.K.), 30 & 31 Vict., c. 3, reprinted in R.S.C. 1985, App. II, No. 5.

Indeed, some commentators suggest that the federal Bill C-54 stands on a dubious constitutional footing, since it purports to regulate the collection, handling, and dissemination of personal information in the private sector as a whole. It is not without accident that the proposed legislation is drafted such that it would apply first to interprovincial undertakings (a federal competency), before applying more broadly to the entire private sector.[109] Similarly, jurisdiction over the workplace generally is divided between the federal and provincial governments according to their areas of particular competence.[110] The following section provides an overview of federal privacy legislation before turning to a review of the applicable provincial privacy framework.

a. *The* Criminal Code

The most significant enacted federal privacy protection provisions are found in the *Criminal Code*.[111] The provisions resemble those found in the American *ECPA*.[112] Specific differences in the statutory language, however, provide a fruitful opportunity to compare and contrast the provisions and the manner in which Canadian courts are likely to apply them.

i. Interception of Private Communications

The closest Canadian equivalent to the *ECPA* is found in the invasion of privacy provisions of the *Criminal Code*, sections 183 to 196. Both pieces of legislation incorporate both civil and criminal liability aspects, and the terms employed, while by no means identical, are similar.

According to section 184(1), "[e]very one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offense and liable to imprisonment for a term not exceeding five years." Two elements of this provision require clarification: (i) what does it mean to "intercept"?; and (ii) what is a "private communication"? Both terms are defined in section 183. First, "intercept" includes "the listen[ing] to, record[ing] or acquir[ing] [of] a communication, or acquir[ing] the substance, meaning or purport

---

[109] According to Bill C-54, *supra* note 103, s. 30(1), the privacy provisions do not apply to organizations—except federal undertakings—which collect, use, or disclose personal information within a province—*i.e.*, the information is not concurrently or subsequently used, collected, or disclosed by the organization in another province—and in which the legislature of the province has the power to regulate the collection, use, or disclosure. According to s. 30(2), s. 30(1) ceases to have effect three years after the day it comes into effect.

The section is cryptic and poorly drafted. Its apparent purpose is twofold: (i) to avoid trampling too heavily on an area of provincial jurisdiction, *i.e.*, by treating federal undertakings *and* interprovincial undertakings (as per the *Constitution Act, 1867*, *ibid.*, s. 92(10)(a)); and (ii) to provide most private corporations sufficient time to implement the required privacy procedures.

[110] See Laperrière & Kean, *supra* note 99 at 713ff.

[111] *Supra* note 44.

[112] For a discussion of the *ECPA*, see Part III.A.2, above.

thereof." Second, "private communication" means "any oral communication, or any telecommunication ... made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it."

It is important to notice that the definition of "intercept" in the *Criminal Code* is potentially broader than the definition of "intercept" in the *ECPA*. This is because interception includes the *acquiring* of a communication, and hence may apply to the listening, recording, or acquiring of stored communication such as e-mail kept on a computer system.[113] One Canadian case, *R.* v. *McQueen*,[114] interpreted the term "intercept" in accordance with its primary dictionary meaning as "an interference between the place of origin and the place of destination of the communication." This interpretation corresponds with the decision of the American court in *Steve Jackson Games*.[115] However, *McQueen* was decided in 1975, before the introduction of the invasion of privacy provisions of the *Criminal Code*. Accordingly, the decision did not take into account the statutory definition of "intercept" which is potentially broader than the dictionary definition of this term.

Moreover, the assessment that a communication is "private" revolves around the characterization of the "expectation of privacy" associated with the nature of the communication. Canadian courts have held that *prima facie* telephone calls are private communications. However, where the circumstances of the conversation are such that the originator of the conversation should have reasonably expected that the conversation would not be private, the conversation is no longer protected.[116] For example, a telephone call to a police switchboard in which the accused threatened the life of a police officer was held not to be a private communication, since it was unreasonable to expect that such a communication would not be listened to or recorded by a person other than the switchboard operator.[117] Similarly, verbal pager messages have been held not to be private communications, since the paging unit plays the message audibly such that anyone in the vicinity of the recipient can hear it.[118] By contrast, the

---

[113] Whereas in the *ECPA* listening is viewed as a form of acquiring, in the *Criminal Code*, listening, recording, and acquiring are set forth in contradistinction one from the other.

[114] (1975), 25 C.C.C. (2d) 262, [1975] 6 W.W.R. 604 (Alta. C.A.) [hereinafter *McQueen*].

[115] *Supra* note 69.

[116] *R.* v. *Solomon*, [1992] R.J.Q. 2631, 77 C.C.C. (3d) 264 (Mun. Ct.) [hereinafter *Solomon*]; *R.* v. *Bengert* (1978), 47 C.C.C. (2d) 457, 15 C.R. (3d) 7 (B.C. S.C.); and *R.* v. *Rodney* (1984), 12 C.C.C. (3d) 195, 40 C.R. (3d) 256 (B.C. S.C.). See also *R.* v. *Newall* (1982), 140 D.L.R. (3d) 184, 69 C.C.C. (2d) 284 (B.C. S.C.) where police used a valid warrant to intercept a cassette recording of a conversation sent by regular postal mail. The court found that the recording was not a "private conversation" (and hence the police did not need a separate warrant for it), as the originator could not have reasonably expected that no one else would ever hear the recording.

[117] *R.* v. *Monachan* (1981), 60 C.C.C. (2d) 286, 22 C.R. (3d) 1 (Ont. C.A.).

[118] *R.* v. *Lubovac* (1989), 101 A.R. 119, 52 C.C.C. (3d) 551 (C.A.); and *R.* v. *Nin* (1985), 34 C.C.C. (3d) 89 (Qc. Mun. Ct.), online: QL (CCC).

caselaw has split on whether there is an expectation of privacy in the use of a cellular phone, in part because of the possibility of interception via the use of a scanner.[119]

Whereas several American decisions have held that e-mail does not carry with it a reasonable expectation of privacy, the Alberta Court of Queen's Bench in *R.* v. *Weir*[120] found that e-mail with the Internet service provider carries a reasonable expectation of privacy. In *Weir*, the court cited with approval *Maxwell*.[121] Note, however, that as yet, no Canadian court has pronounced itself as to whether employee use of e-mail and the Internet carries a reasonable expectation of privacy.

Like the *ECPA*, section 184 of the *Criminal Code* carries with it a number of exceptions. Two exceptions are of particular relevance to our discussion. At section 184(2)(a), it is stated that section 184(1) of the *Criminal Code* does not apply to "a person who has the consent to intercept, express or implied, of the originator of the private communication or of the person intended by the originator thereof to receive it." Moreover, it is stated at section 184(2)(c) of the *Criminal Code* that section 184(1) does not apply to

> a person engaged in providing a telephone, telegraph or other communication service to the public who intercepts a private communication,
>
> (i) if the interception is necessary for the purpose of providing the service,
>
> (ii) in the course of service observing or random monitoring necessary for the purpose of mechanical or service quality control checks, or
>
> (iii) if the interception is necessary to protect the person's rights or property directly related to providing the service.

With respect to the notion of consent, the similarities between the language used in section 184(2)(a) of the *Criminal Code* and *ECPA* § 2511(2)(d) are striking, and American jurisprudence on the subject might prove illuminating. The conclusions of the court in *Watkins*[122]—a case involving an employer's monitoring of an employee's telephone conversations—are apt. The court found: (i) that the employee did not consent to a policy of general monitoring; (ii) that she consented to monitoring of sales calls but not personal calls; (iii) that this consent included the inadvertent interception of a personal call, but only for as long as necessary to determine the nature of the call; (iv) that consent cannot be cavalierly implied; (v) that the strong policy purpose of the

---

[119] Compare *Solomon*, supra note 116 (held there was no expectation of privacy) and *R.* v. *Cheung* (1995), 100 C.C.C. (3d) 441 (B.C. S.C.), online: QL (CCC) [hereinafter *Cheung*] (held there was an expectation of privacy). *Cheung* explicitly refused to follow *Solomon*. Note also that when *Solomon* was considered by the Court of Appeal, the court declined to rule on whether a cellular conversation was "private" within the meaning of s. 184(1), noting only that there was enough of an expectation of privacy to require, on *Charter* grounds, a warrant before such calls could be legally intercepted. See also *R.* v. *Solomon* (1996), 139 D.L.R. (4th) 625, 110 C.C.C. (3d) 354 (Qc. C.A.) [hereinafter *R.* v. *Solomon*].

[120] (1998), 213 A.R. 285, [1998] 8 W.W.R. 228 [hereinafter *Weir* cited to A.R.].

[121] *Supra* note 91.

[122] *Supra* note 71.

privacy protection law would be thwarted if consent could be routinely implied from circumstances; and (vi) that knowledge of the capability of monitoring alone cannot be considered implied consent.

In short, Canadian courts may well pose the question: consent to *what*? That is, what kind of monitoring has the employee agreed to abide by? Moreover, Canadian courts will likely examine the nature of the consent, whether express or implied, to determine whether it was validly and clearly obtained. On this point, two Canadian cases are relevant. In *Duarte*,[123] the Supreme Court of Canada held that there was no logical distinction between third party electronic surveillance and participant surveillance from the perspective of consent. That is, the court found that the consent of one party to the monitoring of a communication in no way remedied the lack of consent of the second party to the communication. Second, the case *R.* v. *Goldman*[124] stands for the position that consent must be freely given, without coercion.

Despite similarities in the language used in the exception to the offense of intercepting private communications as drafted in the *Criminal Code* invasion of privacy provisions and the *ECPA* provisions, there are also significant differences, with the result that American jurisprudence may be largely irrelevant in the Canadian context.

First, the exception applies only to a person engaged in providing a communication service *to the public*. Accordingly, the section does not apply to a private company providing a communication service only to its employees; rather, it is intended to apply to those offering services to the public at large, such as telephone companies, for instance.

Second, the language of the business extension exception at section 184(2)(c) of the *Criminal Code* is narrower than the language of the corresponding *ECPA* exception. Whereas *ECPA* § 2511(2)(a)(i) allows interception in the normal course of employment while engaged in activity which is necessarily incident to the rendition of his service *or* to the protection of the rights or property of the provider, the Canadian exception refers to interception which is necessary "to protect the person's right or property *directly related to providing the service*."[125] In other words, whereas in the *ECPA*, an exception is established whenever monitoring is effected to protect the rights and property of the provider generally, in Canada, the corresponding exception is limited to monitoring effected to protect property "directly related to providing the service."

Accordingly, the so-called "provider exception" at *ECPA* § 2701(c)(1), as discussed in *Bohach*,[126] does not exist in Canadian law. Moreover, the so-called "business extension exception" at *ECPA* § 2510(5)(a)(i), is limited, in Canadian law, to inter-

---

[123] *Supra* note 27.

[124] (1979), [1980] 1 S.C.R. 976, 108 D.L.R. (3d) 17.

[125] *Criminal Code, supra* note 44, s. 184(2)(c)(iii) [emphasis added].

[126] *Supra* note 75.

ception by persons providing communication services *to the public*, for the protection of the person's rights or property *directly related to providing such service.*

ii. Other Criminal Offences

Section 193 of the *Criminal Code* makes it an indictable offence to *disclose* certain information pertaining to intercepted private communications, subject to certain exceptions. The essence of this offence is the making known to another person the existence of an intercepted private communication.

The offence created encompasses three distinct elements. First, the interception must have been made by one of the devices listed, and it must have been done without the consent of either the originator or the person intended to receive it. Second, there must be no express consent of such persons to use information or disclose its contents or meaning as set out in section 193(1)(a) or to disclose its existence. Third, the actions of the accused must be proven to be wilful. Note that merely revealing the existence of the interception is enough; for example, it is irrelevant whether the recording made is in fact fully comprehensible.[127]

Another relevant provision is section 342.1(1)(b) of the *Criminal Code*, which makes it an offence for a person, fraudulently or without "colour of right", to intercept (or cause to be intercepted) either directly or indirectly any computer service by means of any device. As defined in section 342(2), the monitoring of e-mail is implicitly, if not explicitly, encompassed by the technical aspects of the provision, *i.e.*, the definitions of "function" and "intercept". The courts have held in construing these sections that an honestly asserted proprietary or possessory claim constitutes a "colour of right" notwithstanding that it is unfounded in law or fact.[128] While a court might find, for example, that an employer had no right to intercept its employees' e-mail, the employer's honest, albeit mistaken, belief that it did have such a right could suffice to protect it.

In conclusion, while Canadian courts have yet to apply *Criminal Code* provisions to the context of employer monitoring of employee e-mail and Internet use, employers would be prudent to obtain the clear consent of employees to any such monitoring rather than risk the possibility of facing criminal sanctions.

---

[127] *R.* v. *Simm* (1976), 71 D.L.R. (3d) 732, 31 C.C.C. (2d) 322 (Alta. S.C.(T.D.)).

[128] See *R.* v. *Howson*, [1966] 2 O.R. 63, 3 C.C.C. 348; and *R.* v. *Lilly*, [1983] 1 S.C.R. 794, 147 D.L.R. (3d) 758. Note, however, that a moral right alone (or an honest belief therein) cannot of itself find a "colour of right": see *R.* v. *Cinq-Mars* (1989), 51 C.C.C. (3d) 248 (Qc. C.A.), online: QL (AQ); and *R.* v. *Hemmerly* (1976), 30 C.C.C. (2d) 141 (Ont. C.A.), online: QL (CCC).

b. *The* Privacy Act

The federal *Privacy Act*[129] sets forth a series of rules related to the collection of personal information by government institutions. Section 4, for instance, limits the collection of information to such information which has a direct relationship to the programs or activities of the institution in question.

c. *The* Telecommunications Act

One of the stated objectives of the *Telecommunications Act*[130] is "to contribute to the privacy of persons."[131] Pursuant to this objective, the Act grants the Canadian Radio-Television & Communications Commission (CRTC) authority under section 41 to prohibit or regulate the use by any person of the telecommunication facilities of a Canadian carrier for the provision of unsolicited telecommunications. Moreover, Communications Canada has established privacy protection principles applicable to the telecommunications sector.[132]

d. *The* Radiocommunication Act

According to section 6(1)(i) of the *Radiocommunication Act*,[133] the Governor-General may make regulations prohibiting or regulating, in relation to interference to radiocommunication. According to section 9(1)(b), no person shall, without lawful excuse, interfere with or obstruct any radiocommunication. The Act defines a radiocommunication as "any transmission, emission or reception of signs, signals, writing, images, sounds or intelligence of any nature by means of electromagnetic waves of frequencies lower than 3,000 GHz propagated in space without artificial guide."[134]

The Act was amended in 1993 such that it now includes the following privacy protection provisions. According to section 9(1.1):

> [E]xcept as prescribed, no person shall make use of or divulge a radio-based telephone communication
>
> (a) if the originator of the communication or the person intended by the originator of the communication to receive it was in Canada when the communication was made; and

---

[129] R.S.C. 1985, c. P-21. Under the authority of the Act, the federal government has also passed the *Regulations respecting the Privacy Act*, S.O.R./83-13.

[130] *Supra* note 104.

[131] *Ibid.*, s. 7(i).

[132] See Communications Canada, *Principes de protection de la vie privée dans les télécommunications* (Ottawa: Communications Canada, 1992), cited and summarized in Trudel, *supra* note 30 at 11.22, n. 110.

[133] *Supra* note 105.

[134] *Ibid.*, s. 2: "radiocommunication".

> (b) unless the originator, or the person intended by the originator to receive the communication consents to the use or the divulgence.

According to section 9(2), "except as prescribed, no person shall intercept and make use of, or intercept and divulge, any radiocommunication, except as permitted by the originator of the communication or the person intended by the originator of the communication to receive it." Finally, according to section 9.1, every person who contravenes section 9(1.1) or 9(2) is guilty of an offence punishable on summary conviction and is liable, in the case of a person other than an individual, to a fine not exceeding $75,000.

e. *The* Bank Act

The *Bank Act*[135] contains privacy provisions which affect the collection, handling, and dissemination of personal information held by banks. Leaders in private sector privacy protection, the chartered banks have established a voluntary privacy protection code which governs their handling of personal information related to their clients.

f. *The* Canada Labour Code

The working conditions of employees of federal enterprises are regulated by the *Canada Labour Code*.[136] The Code establishes a framework for the negotiation of a collective agreement between unions and employers as well as setting forth certain norms related to working conditions at federal enterprises, whether unionized or not. Laperrière and Kean discuss at some length the various provisions of the Code which impact on privacy protection.[137] For the purposes of this article, their most important conclusion is that very few collective agreements negotiated pursuant to the Code contain privacy protection provisions. Accordingly, the privacy protection of employees has been developed by arbitrators in much the same way as courts develop the common law, most recently seeking guidance from *Charter* values, as will be discussed below.

g. *Bill C-54*

The Federal Government tabled Bill C-54[138] before Parliament on October 1, 1998. If passed, the privacy protection elements of the law will take effect immediately with respect to federal undertakings and will take effect in three years with respect to private corporate entities.[139] While still subject to amendments and while not yet law, several principles contained in Bill C-54 bear direct relevance for our discussion:

---

[135] S.C. 1991, c. 46.
[136] R.S.C. 1985, c. L-2.
[137] *Supra* note 99 at 733ff.
[138] *Supra* note 103.
[139] *Ibid.*, s. 30.

PRINCIPLE 2: *Identifying Purposes.* The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

PRINCIPLE 3: *Consent.* The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

PRINCIPLE 4: *Limited Collection.* The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

PRINCIPLE 8: *Openness.* An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

The Standing Committee on Industry, which has examined Bill C-54 since December 1998, completed its review on March 25, 1999. When it presented its report to the House of Commons on April 13, 1999, the Standing Committee proposed that thirty amendments be adopted. One of the most significant amendments to the Bill is found at section 5(3) which affects Principle 2 set out above. According to section 5(3), "an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances." If and when Bill C-54 is applied to private sector corporations, this reasonability standard will have the effect of forcing employers to justify the scope and rationale underlying their monitoring policies. This principle is closely related to Principle 4 insofar as an employer may well be called upon to justify an unrestricted monitoring of all employee use of company Internet and e-mail tools.

The second set of related principles are Principles 3 and 8. It is on the basis of these two principles—which reflect principles established by the Supreme Court as described above—that employers would be wise not only to outline clearly a policy of acceptable e-mail and Internet use in the workplace, but also to ensure employee consent to these principles prior to use of the tools.

4. Provincial Legislation

a. Common Law Provinces

i. Statutory Torts

A number of Canadian provinces have enacted privacy legislation, which effectively establish a statutory tort for the invasion of privacy. In British Columbia, the

violation of another person's privacy constitutes an actionable tort under the *Privacy Act*.[140] Section 1 of this Act reads as follows:

> (1) It is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another.
>
> (2) The nature and degree of privacy to which a person is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, giving due regard to the lawful interests of others.
>
> (3) In determining whether the act or conduct of a person is a violation of another's privacy, regard must be given to the nature, incidence and occasion of the act or conduct and to any domestic or other relationship between the parties.
>
> (4) Without limiting subsections (1) to (3), privacy may be violated by eavesdropping or surveillance, whether or not accomplished by trespass.

In Newfoundland, the violation of another person's privacy constitutes an actionable tort under *An Act Respecting the Protection of Personal Privacy*.[141] This Act contains provisions similar in part to those in force in British Columbia and in part to those in force in Manitoba:

> 3. (1) It is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of an individual.
>
> (2) The nature and degree of privacy to which an individual is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, regard being given to the lawful interests of others; and in determining whether the act or conduct of a person constitutes a violation of the privacy of an individual, regard shall be given to the nature, incidence, and occasion of the act or conduct and to the relationship, whether domestic or other, between the parties.
>
> 4. Proof that there has been [...]
>
> (b) listening to or recording of a conversation in which an individual participates, or listening to or recording of messages to or from that individual passing by means of telecommunications, otherwise than as a lawful party to them; [...]
>
> without the consent, expressed or implied, of the individual or some other person who has the lawful authority to give the consent is, in the absence of evidence to the contrary, proof of a violation of the privacy of the individual first mentioned.
>
> 5. (1) An act or conduct is not a violation of privacy where
>
> (a) it is consented to by some person entitled to consent;
>
> (b) the act or conduct was incidental to the exercise of a lawful right of defence of person or property; [...].

---

[140] R.S.B.C. 1996, c. 373.

[141] S.N. 1981, c. 6.

The Manitoba *Privacy Act*[142] prohibits one from violating the privacy of another "substantially, unreasonably, and without claim of right."[143] It should be noted, moreover, that in *Ferguson* v. *McBee Technographics Inc.*,[144] the court held that the prohibition against the interception of communications in Manitoba's *Privacy Act* was broader than that encompassed in section 184(1) of the *Criminal Code*.

In *Ferguson*, the court commented on the notion of effective consent for the purposes of lawful monitoring of private communications. The court held that it was an insufficient defence against a claim of invasion of privacy to argue that one party consented to the interception of private communications. According to the court:

> If the other party to the conversation could unilaterally consent to and authorize the third party listening or recording, then the purpose of the legislation would be frustrated and the person whose privacy was sought to be preserved would have no protection at all.[145]

This decision is in accordance with the decision of the Supreme Court of Canada in *Duarte*.[146] There is nothing comparable to section 184(2)(a) of the *Criminal Code* in the Manitoba *Privacy Act* nor in the *Civil Code of Quebec*. Accordingly, the court's findings in *Ferguson* that the plaintiffs could not find lawful authority to their breach of the provisions of the *Privacy Act* in section 184(2)(a) of the *Criminal Code* would likely apply to the Quebec situation as well.

Given the courts' findings in *Duarte* and *Ferguson*, the monitoring of incoming, third party e-mail communications poses a problem from the perspective of privacy protection statutes. Practically speaking, it is virtually impossible to obtain the consent to monitoring of third parties *before* they mail their electronic communication to an employee of a private corporation. Accordingly, the monitoring of such communications is very likely illegal, technically speaking. Two defences to the charge of illegality present themselves.

First, the corporation can protect itself by not monitoring incoming e-mail or by only monitoring the "headers" of incoming e-mail, rather than the content. The monitoring of "headers" and "URL's" to determine where e-mail is going to and coming from, and to determine which web-sites are being accessed by whom, for accounting purposes, will not likely be considered a breach of privacy. This latter information resembles the written address on the outside of an envelope; information, that is, which is traditionally given little to no privacy protection.

Second, the corporation can demonstrate that it has put in place and abides by a reasonable monitoring policy, designed to protect its legitimate proprietary interests and to discourage illegal use of its computer networks, with a minimum invasion of

---

[142] R.S.M. 1987, c. P-125.

[143] *Ibid.*, s. 2(1).

[144] (1989), 58 Man. R. (2d) 119, 24 C.P.R. (3d) 240 (Q.B.) [hereinafter *Ferguson* cited to C.P.R.].

[145] *Ibid.* at 242.

[146] *Supra* note 27.

the privacy of its employees and the public at large. Under such circumstances, it would be less likely that a court would find the corporation liable for breaching the privacy of a third party.

Finally, while the province of Ontario does not have an analogous "Privacy Act", section 112 of the Ontario *Telephone Act*[147] reads as follows:

> Every person who, having acquired knowledge of any conversation or message passing over any telephone line not addressed to or intended for such person, divulges the purport or substance of the conversation or message, except when lawfully authorized or directed so to do, is guilty of an offence.

ii. The *Canada Post Act*

According to section 40(3) of the *Canada Post Act*,[148] no one may open a sealed letter between the time it is sent and the time it is received unless one suspects that the mail is being used to commit an infraction or unless the author or intended recipient consents to the opening. Trudel suggests that the privacy principles contained in telecommunications and postal legislation may serve as guides for an understanding of an individual's reasonable expectation of privacy with respect to e-mail use.[149]

iii. Common Law Tort

It was long held that there is no common law right of privacy in Canada.[150] This appears to have changed. Ontario courts have held that the tort of invasion of privacy exists in common law. *Saccone* v. *Orr*[151] was the first case to acknowledge the common law right to privacy. In this case, the plaintiff sued the defendant for taping a telephone conversation and for then broadcasting it publicly, without prior authorization. Jacob J. held rather tentatively:

> Certainly, for want of a better description as to what happened, this is an invasion of privacy and, despite the very able argument of defendant's counsel that no such action exists, I have come to the conclusion that the plaintiff must be given some right of recovery for what the defendant has done in this case.[152]

---

[147] R.S.O. 1990, c. T-4.

[148] S.C. 1993, c. C-10.

[149] *Supra* note 30 at 11.49.

[150] See *Re Copeland and Adamson*, [1972] 3 O.R. 248, 28 D.L.R. (3d) 26 (H.C.), denying the existence of a common law right to privacy. See also J. Colombo, "The Right to Privacy in Verbal Communication: The Legality of Unauthorised Participant Recording" (1995) 35 McGill L.J. 921 at 924ff.

[151] (1981), 34 O.R. (2d) 317, 19 C.C.L.T. 37 (Co. Ct.) [hereinafter *Saccone* cited to O.R.].

[152] *Ibid.* at 321-22.

Prior to *Saccone*, three Ontario judgments refused to deny the existence of a right of privacy in Canadian common law.[153] More recently, moreover, the common law right to privacy has been confirmed.[154] Given the applicability of *Charter* values to the common law, the latter will no doubt continue to develop in conformity with the former.

b. Quebec

The strongest privacy protection provisions in Canada exist in Quebec. Under section 5 of the Quebec *Charter*,[155] every person has a right to respect for his private life.

i. Quebec *Charter*

Unlike the situation under the Canadian *Charter*, the applicability of the Quebec *Charter* is not restricted to "government action"; it applies to all disputes, whether involving government action or not.[156] Moreover, the Quebec *Charter* is a *quasi*-constitutional document insofar as Quebec laws which violate its provisions may be challenged on that basis.

According to section 5 of the Quebec *Charter*, "[e]very person has a right to respect for his private life." The two leading decisions which have applied this provision are *Godbout*[157] and *Vice-Versa*.[158] The first involves a public law application of the Quebec *Charter*; the second, a purely private law application.

In *Godbout*, the issue was whether a municipal resolution requiring employees to reside within the municipality's territorial limits violated section 5. The municipality argued that section 5 protected either (i) a very limited class of interests related to the individual (such as a physical image), or (ii) certain kinds of confidential information (such as medical records). The Supreme Court rejected this approach to interpreting section 5. While the provision did indeed protect confidential or personal information, "the ambit of the right of privacy has not yet been fully delineated and ... other aspects of 'private life' may ... be found to enjoy the protection of s. 5".[159] The court found that

---

[153] See *Krouse* v. *Chrysler Canada* (1970), 3 O.R. 135 at 136, 12 D.L.R. (3d) 463 at 464 (H.C.); *Burnett* v. *R.* (1979), 23 O.R. (2d) 109 at 115, 94 D.L.R. (3d) 281 at 288 (H.C.); and *Capan* v. *Capan* (1980), 14 C.C.L.T. 191 at 197 (Ont. H.C.), online: QL (OJ).

[154] *Provincial Partitions Inc.* v. *Ashcor Implant Structures Ltd.* (1993), 50 C.P.R. (3d) 497 (Ont. Gen. Div.), online: QL (CPR) (applying the tort of nuisance by invasion of privacy); and *Lipiec* v. *Borsa* (1996), 17 O.T.C. 64, 31 C.C.L.T. (2d) 294 (Ont. Gen. Div.) (recognizing intentional invasion of privacy as actionable in Ontario).

[155] *Supra* note 16.

[156] See *Godbout*, *supra* note 106 at 910.

[157] *Ibid.*

[158] *Supra* note 38.

[159] *Godbout*, *supra* note 106 at 912.

the choice of where to live was so included within the ambit of the right and hence held that the resolution violated section 5.

In *Vice-Versa*, the issue to be decided was whether the publication in an arts magazine of a photograph of a teenager taken in a public place without her permission constituted an actionable breach of her right of privacy. Lamer C.J.C. in dissent, although not on this point, cited La Forest J. with approval in both *Dyment*[160] and *Godbout*,[161] indicating that "the right of privacy can be analysed in similar terms in private law."[162] Applying section 9.1 of the Quebec *Charter*—which holds that rights and freedoms must be exercised in relation to each other, with proper regard for public order, democratic values, and general well-being—the court undertook a balancing exercise between the subject of the photograph's right to privacy and the appellant's freedom of expression and the public's right to information. It held that the right of privacy prevailed, under the circumstances, over other interests; that the breach of privacy constituted a fault; and that the individual was thus correctly awarded damages for the prejudice suffered. For the purposes of this article, the two decisions are significant in that they demonstrate a recent assertion and strengthening of privacy rights, influenced in part by *Charter* values.

ii. The *Civil Code of Quebec*

Under article 35 of the *Civil Code of Quebec* ("C.C.Q."), "[e]very person has a right to the respect of his reputation and privacy. No one may invade the privacy of a person without the consent of the person or his heirs unless authorized by law." Under article 36 C.C.Q.:

> The following acts, in particular, may be considered as invasions of the privacy of a person:
>
> ...
>
> (2) intentionally intercepting *or using* his private communications;
>
> ...
>
> (6) using his correspondence, manuscripts or other personal documents.[163]

Interpreting the expression "private communication" found in article 36 C.C.Q., Marie-France Bich suggests that it could as easily refer to e-mail as to a telephone conversation.[164] Moreover, it should be noted that the language of article 36 C.C.Q.

---

[160] Privacy "is at the heart of liberty in a modern state" (*Dyment*, *supra* note 20 at 427), and it is based "on the notion of the dignity and integrity of the individual" (*ibid.* at 429).

[161] The right of privacy protects, *inter alia*, the "narrow sphere of personal autonomy within which inherently private choices are made" (*Godbout*, *supra* note 106 at 913).

[162] *Vice-Versa*, *supra* note 38 at 605.

[163] Emphasis added.

[164] M.-F. Bich, "Contrat de travail et Code civil du Québec — Rétrospective, perspectives et expectatives" in Service de la formation permanente, Barreau du Québec, *Développements récents en droit*

differs markedly from the language employed in the United States with respect to both the tort of invasion of privacy and the statutory infractions established in the *ECPA*.[165]

First, article 36(2) C.C.Q. speaks of intercepting *or using* private communications, thus rendering the provision much broader than its American counterpart in the *ECPA* (effectively incorporating elements of both Title 1 and Title 2 of the *ECPA*). Second, article 36(6) C.C.Q. mentions the "use" of correspondence, manuscripts or other documents. This means that e-mail stored in a computer, and hence not technically intercepted by an employer in the context of monitoring, would likely be covered by the provisions of the C.C.Q. Third, there is no explicit mention of an "expectation of privacy" nor of a "highly objectionable" breach of one's privacy rights, unlike the American invasion of privacy tort. Accordingly, the argument and conclusions of the court in *Smyth*[166] do not apply in Quebec.[167]

iii. *Personal Information Protection Act*

The Quebec government enacted *An Act respecting the Protection of Personal Information in the Private Sector*[168] in 1993. The Act complements similar Quebec public sector privacy legislation[169] as well as provides further detail to similar provisions set forth at articles 37 to 41 of the C.C.Q. Sections 4 to 6 of the *Personal Information Protection Act*[170] resemble greatly the provisions of Bill C-54:[171]

---

du travail (1996) (Cowansville, Qc.: Yvon Blais, 1996) 189 at 236. Bich undertakes a thorough analysis of art. 36 C.C.Q. in the context of disputes between employees and employers as regards a violation of privacy rights: see *ibid.* at 233-40.

[165] *Supra* note 66.

[166] *Supra* note 87.

[167] Note that a comment by Moisan J. in *Roy* v. *Saulnier*, [1992] R.J.Q. 2419, 102 D.L.R. (4th) 234 (C.A.) [hereinafter *Roy*] suggests tbat an employee cannot reasonably expect that her business telephone calls would not be monitored. The argument is of little precedential weight, however, because it was made in *obiter*, and prior to the introduction of the C.C.Q., which contains the above-mentioned privacy provisions as well as a prohibition, at art. 2858 C.C.Q., against the use of evidence "obtained under such circumstances that fundamental rights and freedoms are breached." *Syndicat des Employées et Employés du C.L.S.C. Les Forges et Centre Local de Services Communautaires Les Forges*, [1997] T.A. 667 (Durand) [hereinafter *Les Forges*], which cites *Roy* with approval on the matter of admissibility of recorded telephone conversations, is not conclusive on the issue of privacy, since in *Les Forges*, the employer informed the employee that his conversations were recorded. More recently, in *Houle* v. *Mascouche (Ville de)*, [1998] R.J.Q. 466 (Sup. Ct.), online: QL (AQ) [hereinafter *Houle*], the Superior Court of Quebec held that illegally-recorded telephone conversations were not admissible in the wrongful dismissal case, since the admission of evidence obtained in violation of a fundamental right of privacy would bring the administration of justice into disrepute. The decision provides a thorough review of jurisprudence and doctrine on the subject.

[168] S.Q. 1993, c. P-31.1 [hereinafter *Personal Information Protection Act*].

[169] *An Act respecting Access to Documents Held By Public Bodies and the Protection of Personal Information*, R.S.Q. c. A-2.1.

[170] *Supra* note 168.

4. Any person carrying on an enterprise who may, for a serious and legitimate reason, establish a file on another person must, when establishing the file, enter its object.

5. Any person collecting personal information to establish a file on another person or to record personal information in such a file may collect only the information necessary for the object of the file.

   Such information must be collected by lawful means.

6. Any person collecting personal information relating to another person may collect such information only from the person concerned, unless the latter consents to collection from third persons.

These provisions contain several of the same privacy principles discussed above, namely, identifying reasonable purposes, consent, and limited collection. Any one or all of these could apply in Quebec to the monitoring of employee e-mail and Internet use by employers. Once again, the existence of such principles argues in favour of either obtaining employees' consent prior to monitoring or reserving monitoring to exceptional circumstances where the employer has reason to believe the employee has committed a wrongdoing of some sort. Even in the latter situation, it may be more appropriate for the employer to seek the assistance of proper authorities if criminal behaviour is suspected.

IV. Electronic Privacy in the Employment Context: Competing Interests

As discussed above, the right of privacy is not absolute. Under certain circumstances, the right must yield to competing interests. In the workplace context, such interests include the employer's right of direction and control, the employee's duty of loyalty, as well as the employer's right of ownership. These concepts are discussed here briefly in the abstract before being examined more concretely in the context of disputes between employers and employees with respect to collective bargaining or under an individual contract of employment.

A. The Right of Direction and Control

According to article 2085 C.C.Q., "[a] contract of employment is a contract by which a person, the employee, undertakes for a limited period to do work for remuneration, *according to the instructions and under the direction and control of another person, the employer.*"[172] This right of direction and control is analogous to rights accorded to employers under the common law. It should be noted, however, that quite apart from any limits imposed on this right by countervailing employee rights—such as the right of privacy or dignity—the right of direction and control is also subject to

---

[171] *Supra* note 103.

[172] Emphasis added.

an inherent limitation: employer directives and surveillance must be effected in direct relation to the carrying out of obligations as set forth in the contract of employment.[173]

An employment contract, by its very nature, creates a relationship of subordination. To ensure the efficient and profitable functioning of an enterprise, employers have a right of direction and control over their employees. Employers assign work tasks in accordance with the terms of the employment contract and any applicable employment legislation and have the right to ensure that the tasks are adequately undertaken. Employers thus have a right to reprimand an employee who wastes an inordinate amount of time browsing the Internet or writing e-mail to friends, rather than working to complete an assigned task. Similarly, employers have the right to reprimand acts of insubordination such as situations where an employee speaks openly and negatively of a "superior".[174]

B. The Duty of Loyalty

Often expressed as an employee's obligation rather than as an employer's right, employees owe their employer a duty of loyalty. This duty involves a certain commitment to the employer to work faithfully on the employer's behalf, as well as an undertaking not to divert or solicit the employer's customers or employees on behalf of a third party. The duty may even survive the end of en employment contract if the contract contains a non-competition clause.[175] Such clauses, however, must be limited in geographical scope, duration, and sphere of economic activity so as to ensure that the employee maintains a means of earning a livelihood in the event of a termination of the employment contract. In other words, the duty itself is inherently limited. As will be discussed below, electronic surveillance is often employed as a means of demonstrating that an employee has breached his duty of loyalty.[176]

C. Ownership Rights

Employers generally hold ownership rights over not only office equipment, but more importantly in the context of employee monitoring of employee e-mail and Internet use, over intellectual property. In an information economy, intellectual property is often one of an enterprise's most valuable assets. The very virtues of the Internet—the collapsing of distance, ease of communication, low cost, ease of producing infinite numbers of perfect copies of digital information—can have vicious consequences if the technology is misused. Employers have reason to fear inappropriate transmission, whether deliberate or inadvertent, of confidential and/or proprietary in-

---

[173] See C. D'Aoust, "L'électronique et la psychologie dans l'emploi" in D. Nadeau & B. Pelletier, eds., *Relation d'emploi et droits de la personne : évolution et tensions!* (Cowansville, Qc.: Yvon Blais, 1994) 35.

[174] See *e.g. Smyth, supra* note 87.

[175] Art. 2089 C.C.Q.

[176] See *e.g. Houle, supra* note 167.

formation. Confidential information, trade secrets, copyrighted or patented materials; any or all of these things can be copied and transferred with ease over the Internet and employers demonstrate justifiable concern for this fact. As indicated above, however, property rights alone are insufficient to negate employee privacy rights.[177]

D. Avoidance of Liability

On the basis of principles of vicarious liability, employers can be held liable for the misdeeds effected by employees in the course of employment. In the context of Internet and e-mail use, such misdeeds may include posting or downloading illegal materials, such as child pornography,[178] violating the copyright of a third party, or harassing a third party via e-mail.[179] Employers are justifiably concerned by such phenomena and have a direct interest in ensuring that such misuse of e-mail and the Internet does not occur in the workplace.

---

[177] In *Re Saint Mary's Hospital (New Westminster) and H.E.U.* (1997), 64 L.A.C. (4th) 382 (Larson) [hereinafter *Saint Mary's*], the employer hospital surreptitiously installed a video surveillance camera in the ceiling of an employee's office to monitor employees suspected of theft. While the arbitrator found that the employer had a right to protect its property against a "serious problem of vandalism and theft" (*ibid.* at 399), he nonetheless held that the employer had inappropriately breached employee privacy rights, since other less intrusive means of protecting the employer's property should have been employed:

> What must be kept clearly in mind in these kinds of cases, however, is that the right to privacy is a basic human right which must not only be guarded but which must also be nurtured through mutual respect and understanding. The privacy of a group of employees is so important that an employer must do everything reasonably possible to secure its property before it is entitled to initiate clandestine surveillance (*ibid.* at 400).

Moreover, *Re Brampton Hydro and C.A.W., Loc. 1285* (1991), 23 L.A.C. (4th) 126 (Hughes) provides a fact pattern which is analogous in many ways to the monitoring of e-mail. Brampton Hydro suspended a lineman for three days for failing to hand over or open an inter-office envelope and for leaving the service centre when told not to. The lineman claimed that the envelope contained personal information. In fact, it contained a company bulletin. In dismissing the employee's grievance, the arbitrator held that the employee's privacy rights were not breached because the envelope did not contain any "personal property". Had the contents of the envelope been personal, the employee would have been justified, according to the arbitrator, in refusing the search.

In a similar vein, Philip Zimmerman, creator of P.G.P. (Pretty Good Privacy) encryption technology, cited in P.D. Samuels, "Increasingly, Companies Deny Employees Privacy Rights in E-mail" *The New York Times* (11 May 1996), online: The New York Times <http://www.nytimes.com/library/cyber/week> (date accessed: 24 October 1998) asks rhetorically: "If I use [a company pen] to write a letter to my wife, does that mean they can read the letter?"

The main point in this and other cases is that property rights and privacy rights are not mutually exclusive. While the "physical plant", whether it be a computer system or a factory, may belong to the employer, still there remains a private realm of the employee within the employer's property which the employer must respect.

[178] See *e.g. Weir, supra* note 120.

[179] See *e.g. Di Vito* v. *Macdonald Dettwiler & Associates* (1996), 21 C.C.E.L. (2d) 137 (B.S. S.C.), online: QL (BCJ) [hereinafter *Di Vito*].

V. Electronic Privacy in the Employment Context: Converging Interests

A. Autonomy

In an information economy, employee autonomy is an asset. The rapid pace of technological change that characterizes our economy requires employees who are creative, independent, and who strive toward life-long learning.[180] If employees feel that every statement they make is recorded, every gesture monitored, they will inevitably curtail their experimentation. As Harlan J. wrote in *White*[181] of a form of electronic surveillance (bugging):

> [W]ords would be measured a good deal more carefully and communication inhibited if one suspected his conversations were being transmitted and transcribed. Were third-party bugging a prevalent practice, it might well smother that spontaneity—reflected in frivolous, impetuous, sacrilegious, and defiant discourse—that liberates daily life.

B. Healthy Working Environment

Concerns about sexual harassment[182] or racist behaviour[183] by employees using e-mail are shared by both employers and employees. Inappropriate comments may have a serious detrimental effect on the psychological well-being of the employee(s) who are subjected to such comments. Employers and employees alike, therefore, have an interest in ensuring that such inappropriate behaviour is not left unchecked.

Similarly, employers and employees alike have a mutual interest in ensuring that the workplace environment is as pleasant as possible. Unwarranted or overzealous monitoring may have a deleterious impact on working conditions.[184] As Tom Wright writes:

---

[180] See D. Tapscott, *The Digital Economy: Promise and Peril in the Age of Networked Intelligence* (New York: McGraw-Hill, 1996).

[181] *Supra* note 45 at 787-89, cited in *Duarte*, *supra* note 27 at 54.

[182] See *Di Vito*, *supra* note 179; and *Rudas* v. *Nationwide Mutual Ins. Co.*, 73 Fair Empl. Prac. Cas. (BNA) 187 (E.D. Pa. 1997), online: LEXIS (GENFED/MEGA) (sexual harassment via e-mail), cited in Lomax, *supra* note 3.

[183] See *Owens* v. *Morgan Stanley & Co.*, 74 Fair Empl. Prac. Cas. (BNA) 876 (S.D.N.Y. 1997), online: LEXIS (GENFED/MEGA) (racist comments via office e-mail), cited in Lomax, *ibid.*

[184] In *Re Liberty Smelting Workers (1962) Ltd. and U.A.W., Loc. 1470* (1972), 3 S.A.G. 1039 (Dulude), an employer installed a closed circuit television in a factory on a temporary basis in order to prevent theft. The labour arbitrator wrote in his decision:

> [Translation] There is no doubt in my mind, that unless there are contrary express or implicit provisions in the contract, the employer cannot use close circuit television for disciplinary or other reasons.

> [W]hen invasions of privacy occur, employees often feel that self-worth, morale, and the over-all quality of working life are eroded. The ensuing negative impact of invasions of privacy on work quality and productivity is hidden human and real costs (*e.g.* absenteeism and employee compensation claims), not often calculated by employers.[185]

VI. Applying Privacy Rights to Workplace Surveillance: Two Contexts

A. *Collective Agreements*

1. Interpreting Collective Agreements

Traditionally, as discussed more fully by Beth Bilson,[186] arbitrators have looked to the "management prerogative" or "management rights" clause of a collective agreement when addressing grievances by employees with respect to employer practices regarding searches and inspections. In some instances, the agreement contains specific provisions, outside the management rights clause, regarding searches and surveillance, although this is rare.[187] In other instances, the management rights clause itself contains explicit limitations on the employer's right to conduct searches, although this too is rare.[188] Most commonly, arbitrators must interpret the management rights clause provisions which simply indicate that the employer explicitly reserves the power to make rules and policies for the governance of the workplace, or, where such a reserve is not explicit, arbitrators have "read in" such a reserve on the basis of a "residual rights theory"—*i.e.*, whatever rights are not removed under the collective agreement remain with the management.

According to Bilson, when interpreting such rights, arbitrators traditionally contemplated various minimal restrictions to management prerogatives as summarized in

---

> The worker-employee is neither a robot nor a slave; he was hired by contract to devote his time and energy to his employer to accomplish his work. At all times and in all places, he maintains his human dignity, his individual liberty.
>
> It is repugnant to think that during the course of daily operations of his work, he is constantly under the electronic observation of cameras directed toward him, that all of his sightless gestures are recorded in continuous fashion, as if he were under a microscope (*ibid.* at 1044-45).

[185] T. Wright, *Privacy Makes Good Business Sense* (Toronto: Information and Privacy Commission, 1994) at 2.

[186] See B. Bilson, "Search and Surveillance in the Workplace: An Arbitrator's Perspective" in W. Kaplan, J. Sack & M. Gunderson, eds., *Labour Arbitration Yearbook 1992* (Toronto: Butterworths, 1992) 143 at 145ff.

[187] See *e.g. Re Drug Trading Co. & Druggists' Corp.* (1988), 32 L.A.C. (3d) 443 (Foisey).

[188] See *e.g. Re Lornex Mining Corp* (1983), 14 L.A.C. (3d) 169 (Chertkow).

Re KVP Co.[189] The restrictions focused on the notion of reasonableness in the substance and implementation of a given workplace rule. "Using this approach to a grievance related to a search or inspection, the inquiry of the arbitrator would be directed toward such factors as the notice given to the employee of the search policy, the clarity of the policy or the fairness of the administration of the policy."[190]

Moreover, according to Bilson, it was once controversial whether arbitrators could consider the relationship between a collective agreement and relevant statutory provisions when attempting to resolve a dispute between management and unions. The Supreme Court of Canada resolved the controversy in *McLeod* v. *Egan*,[191] holding that its arbitrators not only could, but should, on occasion, look to relevant statutory provisions for assistance in interpreting a collective agreement. In *Re Canada Post Corp. (Fingerprinting Grievance)*,[192] the arbitrator reviewed provisions not only of the *Criminal Code*[193] with respect to criminal procedure, but also provisions of the federal *Privacy Act*[194] and the *Canadian Human Rights Act*[195] to determine whether Canada Post had the right to fingerprint its employees.

More recently, so-called "*Charter* values" regarding the respect of personal privacy have influenced the results in a number of labour arbitration cases.[196] In *Re Doman Forest Products Ltd. and I.W.A., Loc. 1-357*,[197] for instance, a labour arbitrator was called upon to determine the admissibility of video surveillance in a case of wrongful dismissal. The case involved an employer who, suspecting that an employee was abusing sick leave, hired a private investigator to monitor the absent employee. The employee was dismissed. Citing *Dolphin Delivery*[198] as authority, the arbitrator wrote:

> [I]t seems to me that while s. 8 of the *Charter* does not apply to this dispute, as an adjudicator, I am called upon to bear in mind those fundamental *Charter* values now articulated by the Supreme Court in *R.* v. *Duarte* and *Hunter* v. *Southam*. ... The values extracted from those decisions are clear. Electronic surveillance *by the state* is a breach of an individual's right to privacy and will only be countenanced by application of the standard of reasonableness enunciated in *Hunter* v. *Southam Inc.* ... I must now relate those values to the realm of

---

[189] (1965), 16 L.A.C. 73 (Robinson).

[190] Bilson, *supra* note 186 at 145-46.

[191] [1975] 1 S.C.R. 517, 46 D.L.R. (3d) 150 [hereinafter *Egan* cited to S.C.R.].

[192] (1988), 34 L.A.C. (3d) 392 (Bird).

[193] *Supra* note 44.

[194] *Supra* note 129.

[195] R.S.C. 1985, c. H-6.

[196] See also C.L. Rigg, "The Right to Privacy in Employment: An Arbitrator's Viewpoint" in W. Kaplan, J. Sack & M. Gunderson, eds., *Labour Arbitration Yearbook 1991* (Toronto: Butterworths, 1991) 83.

[197] (1990), 13 L.A.C. (4th) 275 (Vickers) [hereinafter *Doman*].

[198] *Supra* note 49.

> a private dispute between an employer and an employee whose relationship is governed by the terms of a collective agreement.[199]

In applying the *Charter* values, the arbitrator found that, despite the fact that the collective agreement did not contain specific provisions which guaranteed a right of privacy, it was nonetheless necessary to weigh the employee's right to privacy against the company's right to investigate what it considered to be an abuse of sick leave. According to the arbitrator, a number of questions had to be answered, including was it reasonable, under the circumstances, to request surveillance? Was the surveillance conducted in a reasonable manner? Were there alternatives open to the company to obtain the evidence it sought? The arbitrator decided to hear the evidence subject to union objections regarding admissibility which would be ruled upon in the final award. After hearing the evidence, the arbitrator ruled the videotapes inadmissible.

In *Re Steels Industrial Products*,[200] the labour board referred to *Doman* and to *R.* v. *Wong*[201] and affirmed an employee's right to privacy as follows:

> As a general principle, I would not think that a private citizen—specifically here an employer—should have greater freedom or authority to monitor another private citizen than does the state, even if the private citizen is one's employee. ... [G]reat circumspection is called for when an employer seeks to electronically monitor the activity of an employee off the job—albeit during otherwise working hours. The employer-employee relationship is based on an employment contract and the videotaping of an employee clearly is at the extreme of the employer's authority under such a contract.[202]

The labour board in *Steels* adopted the test set forth in *Doman* and concluded that the surveillance was justified.[203]

In *Re Labatt Ontario Breweries (Toronto Brewery) and Brewery, General and Professional Workers Union, Loc. 304*,[204] the employer challenged the logic of *Doman* and the cases which have followed it, at least insofar as the principles have been applied in Ontario. The employer questioned whether an arbitrator can apply *Charter* values in a private dispute between an employer and an employee, recalling the controversy over statutory interpretation which *Egan*[205] purported to resolve. The company argued that *Dolphin Delivery* stands for the proposition that the "judiciary" is entitled to apply *Charter* values to a dispute between private litigants; arbitrators are not similarly empowered. The arbitrator agreed that "in the Province of Ontario at least, arbitrators have no jurisdiction to apply the *Canadian Charter of Rights and*

---

[199] *Supra* note 197 at 279 [emphasis in original].

[200] (1991), 24 L.A.C. (4th) 259 (Blasina) [hereinafter *Steels*].

[201] [1990] 3 S.C.R. 36, 60 C.C.C. (3d) 460 (unreasonable search and seizure).

[202] *Steels, supra* note 200 at 274.

[203] See also *Re Toronto Star Newspapers Ltd. and Southern Ontario Newspapers Guild* (1992), 30 L.A.C. (4th) 306 (Springate); and *Saint Mary's, supra* note 177.

[204] (1994), 42 L.A.C. (4th) 151 (Brandt) [hereinafter *Labatt*].

[205] *Supra* note 191.

Freedoms, either directly or indirectly, to a dispute under a collective agreement between litigants who ... are private contracting parties."[206] Nonetheless, the arbitrator found that employees under a collective agreement enjoy a legally protected right to privacy quite apart from any *Charter* considerations. The arbitrator concluded:

> Although I have rejected the argument in *Domtar* ... and *Steels* ... that the foundation for the right to privacy rests in the *Charter*, I nonetheless find it helpful to use those cases as a guideline for determining how best the balance between employer and employee interests should be struck.[207]

Recently, in *L'Union des routiers*,[208] the arbitrator was seised with a union grievance involving the installation of hidden video cameras in a locker room. Significantly, both parties to the dispute were in agreement as to the principles which applied in a case of a deemed breach of employee privacy rights.[209] The arbitrator cited the following passage from *Labatt* with approval as the governing principle: "[T]he employer's right to investigate suspected wrongdoing must yield to the employee's right to personal privacy unless there is a real and substantial suspicion of wrongdoing and only so long as the search is conducted reasonably."[210] Moreover, the arbitrator, citing the following passage from *Saint Mary's*[211] with approval, indicated that there must be a direct relationship between the use of electronic surveillance and the likelihood of resolving the employer's inquiry: "The onus is on the employer to justify the encroachment upon the employees' right to privacy by demonstrating that there is a substantial problem and that there is a strong probability that surveillance will assist in solving the problem."[212]

Accordingly, a sort of consensus seems to have been reached as to the principles applicable to disputes involving workplace surveillance and privacy: employers must balance an employee's right to privacy and an employer's right of surveillance in accordance with *Charter* values. The consensus is all the more remarkable when one considers that it spans arbitration decisions from British Columbia—a common law province with statutory privacy protection—through Ontario—a common law province with common law privacy protection—to Quebec—a civil law province with *quasi*-constitutional privacy protection.

Treating the issue of electronic surveillance, Brown and Beatty conclude:

---

[206] *Labatt*, *supra* note 204 at 160.

[207] *Ibid.* at 164. Interestingly, in *L'Union des routiers, brasseries, liqueurs douces et ouvriers de diverses industries, Local 1999 et la Brasserie Labatt (Montréal)* (11 January 1999), T.A. 99-00742, Ref. 99T-402 (Foisy) [hereinafter *L'Union des routiers*], the arbitrator cites both *Domtar* and *Labatt* with approval, apparently oblivious to their divergences.

[208] *Ibid.*

[209] See also J.D. Gagnon, "La gestion du personnel : nouvel équilibre des droits des salariés et la direction de l'entreprise" in A. Poupart, ed., *Le Respect de la vie privée dans l'entreprise : de l'affirmation à l'exercice d'un droit* (Montreal: Thémis, 1995) 19.

[210] *Supra* note 204 at 161.

[211] *Supra* note 177.

[212] *Ibid.* at 399.

> [E]ven apart from provisions of the collective agreement which guarantee the maintenance of working conditions, it has been said that both the way in which, and the purpose for which, [electronic surveillance] devices are deployed will figure critically on the extent to which they invade the employee's personal privacy and, accordingly, on the legitimacy of their use.[213]

2. A Hierarchy of Privacy Rights?

Labour arbitrators have been called upon to review a vast array of situations involving search and surveillance and their potential impact on employee privacy rights. Recalling the framework of analysis set forth by La Forest J. in *Dyment*,[214] it is possible to identify three categories of personal privacy interests: personal, territorial, and informational. In the workplace context, all three are potentially present. Drug testing, fingerprinting, and body searches in the workplace context recall the first category. Searches of employees' personal effects, such as those found in desks, filing cabinets, lockers, or lunch pails for instance,[215] recall the second category. The use of personal information obtained from the employee through employment application forms, through monitoring of e-mail and general video surveillance for instance, recall the third category.

In *Saint Mary's*, the arbitrator attempted to synthesize a number of previous arbitration decisions on the subject of privacy by establishing a sort of hierarchy of privacy rights.[216] At the top of the hierarchy—*i.e.*, those searches which are most invasive of privacy—the arbitrator placed searches which involve actual bodily intrusions. Second in order of importance, according to the arbitrator, came those actions which involve searches of personal effects and spaces. Third came "surveillance" cases—the reference seems to be to video surveillance, but might include other forms of electronic monitoring. Moreover, within this last category the arbitrator delineated subcategories: (i) surreptitious surveillance, which has the greatest potential to affront the privacy rights of employees; (ii) open surveillance to protect the security and property of both employer and employees; and (iii) "benign surveillance", what the arbitrator found to be the least intrusive form of electronic surveillance, used for the benefit of employees—*e.g.* videotaping work activities for the purposes of training or to assist temporarily disabled supervisors.

Where would monitoring of employee e-mail and Internet use fit on the scale? The answer would seem to depend on the circumstances. If the monitoring occurs surreptitiously, for instance, then it may fall in the first sub-category of the third category.

---

[213] *Canadian Labour Arbitration*, 3d ed. (Aurora, Ont.: Canada Law Book Inc., 1999) at 7.183 [footnotes omitted].

[214] *Supra* note 20.

[215] See *e.g.* the list of jurisprudence in Brown & Beatty, *supra* note 213 at 7.183, para. 7:3625, n. 20. See also E. Palmer & B. Balmer, *Collective Agreement Artibration in Canada*, 3d ed. (Toronto: Butterworths, 1991) at 340.

[216] *Saint-Mary's, supra* note 177 at 396-99.

If one accepts the analogy that e-mail is like personal mail and that virtual space is like physical space, then monitoring of e-mail use resembles monitoring falling into the second category. By contrast, if monitoring is carried out in accordance with a policy to which the employees have given their consent, and if the purpose of the monitoring is to ensure that the computer server is not overcharged with downloaded computer files (such as video files), then the monitoring might fall into the third sub-category of the third category. Similarly, if the monitoring is done on the basis of a complaint that an employee has been sending e-mail to another employee which may constitute a form of sexual harassment, then the monitoring may fall into the second sub-category of the third category.

Finally, in *Plant*,[217] Sopinka J. explored the concept of a "reasonable expectation of privacy" *vis-à-vis* the various types of information. He held that whereas it is generally possible to base a section 8 Canadian *Charter* claim with respect to information of a purely personal or confidential nature, such is not generally the case of documents of a commercial nature. He writes:

> In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the *Charter* should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual. The computer records investigated in the case at bar while revealing the pattern of electricity consumption in the residence reveals very little about the personal lifestyle or private decisions of the occupant of the residence. ...
>
> This is not to suggest that records prepared in a commercial context can never be subject to the privacy protection afforded by s. 8 of the *Charter*. If commercial records contain material which meets the "personal and confidential" standard set out above, the commercial nature of the relationship between the parties will not necessarily foreclose a s. 8 claim.[218]

While it is difficult to assess the content of an e-mail message or a computer file without reading it, it is nonetheless possible to gain a sense of the content on the basis of a review of its location on the computer or by an examination of the address or URL employed. For instance, if the computer file is located in a sub-directory named "Personal" or "My Documents", then it is more likely to be personal (and hence private) than if it were located in a file related to a specific client or customer. Similarly, if the e-mail message is addressed to a customer or a supplier, one may assume that the content of the message is commercial in nature. Such factors may influence a court when it comes to the determination of whether the employer's application of a monitoring policy was appropriate or not.

---

[217] *Supra* note 32.

[218] *Ibid.* at 293-94. See also *R.* v. *Solomon*, *supra* note 119.

B. Individual Employment Contracts

1. E-mail, the Internet, and Evidence

There has been relatively little case law that has explored the concept of privacy rights in the context of a contract of employment. Most of the cases which provide clues as to how courts will treat the issue stem from objections raised by litigants as to the admissibility of evidence obtained in violation of a privacy right. These cases are equivocal in terms of defining the extent to which employees benefit from privacy protection while on the job, although here again courts have recently tended to afford a much greater deference to privacy rights than they have in the past.

In *Roy*,[219] the appellant suspected that an employee was committing acts of disloyalty by encouraging the appellant's clients to his own competing business. The appellant recorded the employee's telephone calls without obtaining the latter's consent. The issue before the Quebec Court of Appeal was whether the recording was admissible. The court held that it was. Decided prior to the introduction of articles 36 and 2858 C.C.Q., the court found that the evidence was admissible on the basis of a test for the admissibility of mechanical recordings first set forth in *Cadieux* v. *Le Service de Gaz Naturel Laval Inc.*[220] Even if obtained illegally or in violation of the employee's rights under section 5 of the Quebec *Charter*, the evidence was admissible on the basis of that test. The court highlighted the fact that section 49 of the Quebec *Charter*, unlike section 24(2) of the Canadian *Charter*, does not prohibit the introduction of evidence obtained in violation of a fundamental right. It is worth noting, however, that the court found in *obiter* that no privacy right was in fact violated since the subject matter of the conversations was purely commercial.

On very similar facts, the Quebec Superior Court came to very similar conclusions in *Compagnie d'Assurances Standard Life* v. *Rouleau*.[221] Remarkably, despite the applicability of articles 36 and 2858 C.C.Q. to the case at hand, the Superior Court did not feel compelled to alter the analysis put forth by the Court of Appeal in *Roy*.[222] As in *Roy*, however, the Superior Court indicated that the recording did not treat elements of the employee's private life; it was purely commercial.

More recently, however, there appears to have been a shift toward a greater appreciation for employee privacy rights in the context of employment, due in part, perhaps, to the increasing body of Supreme Court jurisprudence which serves to highlight and strengthen the importance of privacy rights in a modern democracy.

---

[219] *Supra* note 167.

[220] [1991] R.J.Q. 2490, 42 Q.A.C. 64.

[221] [1995] R.J.Q. 1407 (Sup. Ct.) [hereinafter *Standard Life*].

[222] See Bich, *supra* note 164 at 235 for further criticism of this judgment.

In *Ouellet* v. *Cuisirama Inc.*,[223] the plaintiff was the ex-employee of her husband. The latter contested the admissibility of a telephone conversation between himself and his wife that the latter recorded without his knowledge. The objection was based on the fact that the recording constituted an invasion of his privacy in breach of articles 3, 35 and 36 C.C.Q. and hence that the evidence should be excluded on the basis of article 2858 C.C.Q. The labour commissioner excluded the evidence: "[L]es nouvelles régles ne permettent pas le dépot de cet élément de preuve qui risque de porter atteinte a la vie privée."[224] In this case, the evidence presented to the court contained content of both a personal and commercial nature. So as to protect the integrity of the evidence admitted, the commissioner decided that it would be inappropriate to edit the recording so as to present only the commercial contents of the recording. The analysis is more satisfactory than that set forth in *Standard Life*.[225] Interestingly, in *Ouellet*, it is the employer who benefits from the invocation of his right of privacy.

More recently, in *Houle*,[226] the Superior Court of Quebec revisited the question of the admissibility of evidence obtained in violation of an individual's right of privacy. A particularly nosey neighbour recorded the plaintiff's telephone conversations at home by means of a scanner. The neighbour then submitted the recordings to the plaintiff's employer, a municipality, which proceeded to fire the plaintiff on the basis of their contents. The Superior Court was called upon to determine the admissibility of the recordings. Rejecting the employer's argument—based on *Roy* and *Standard Life*—that even evidence obtained in violation of a fundamental right was admissible in court so long as its authenticity and probative value can be determined, the Superior Court rejected the evidence. According to the court, article 2858 C.C.Q. is a copy of section 24 of the Canadian *Charter* and hence has the same effect on admissibility of evidence in Quebec private, civil law disputes as does the Canadian *Charter* in cases involving government action.[227] It would thus appear that henceforth, in Quebec at least, evidence obtained in violation of the right of privacy is, in principle, inadmissible.

2. Applying *Charter* Values to Workplace Monitoring

As mentioned above, *Charter* values have had an impact on the outcome of workplace privacy disputes involving individual employment contracts. In situations involving private litigants, moreover, privacy is not a constitutional right, but rather a common law or statutory right whose nature and scope may be interpreted in light of constitutional values.

In the absence of direct case law on the subject of privacy rights in the context of employer monitoring of employee e-mail and Internet use, how might *Charter* values

---

[223] [1995] C.T. 203 (Boisclair) [hereinafter *Ouellet*].

[224] *Ibid.* at 209.

[225] *Supra* note 221.

[226] *Supra* note 167.

[227] See also *Thibodeau* v. *Commission municipale de Québec*, [1996] R.J.Q. 1217 (Sup. Ct.).

influence a court's interpretion of the respective rights of employees and employers? The following factors may help courts, employers, and employees determine whether an employee's action is purely private or carried out in the course of his duties, and hence whether employer monitoring is in breach of a privacy right or not.

a. Location

The distinction between public and private space is a fluid one, as is the distinction between "work space" and "private space". Just as in certain circumstances it may be appropriate for an employer to concern himself with the activities of an employee who has stayed home from work[228] (duty of loyalty, abuse of sick leave), for instance, so too it is at times inappropriate for the employer to monitor an employee's activities while at work.[229] Certain physical locations in work spaces are deemed private. The most obvious examples of such private space are washrooms or shower rooms.[230] This concept of private space may be broadened, however, to include lunch rooms,[231] lockers and locker rooms,[232] filing cabinets, and desks.[233]

What of "virtual space"? On analogy, can it be said that an office computer may contain both work space and private space? Should an employer be able to monitor the content of files contained in a sub-directory marked "My Documents", "My Files", or "Personal" in just the same way that he may access and review files in sub-directories which are clearly work-related? If so, why? Given that an employer's right of direction and control is limited to the furtherance of the obligations of service established pursuant to the employment contract, it would seem inappropriate for an employer to monitor such files without first justifying such surveillance in terms of the employment contract itself.

---

[228] See *e.g. Bridgestone/Firestone Canada Inc. et Syndicat des Travailleuses et Travailleurs de Bridgestone/Firestone de Joliette*, [1995] T.A. 505 (Trudeau).

[229] Deleury & Goubau, *supra* note 43 at 140-41:

> La vie privée ne se réduit pas à la seule protection de la demeure privée. La protection de la loi couvre la vie privée meme en dehors de ce lieu. ... Elle s'étend également aux conversations et communications privées de maniere globale à tout lieu considéré comme privé. ... Les auteurs s'entendent cependant généralement pour considérer que les éléments de la vie privée doivent etre sauveguardés, en tant que tels, des lors qu'ils ne se ratachent pas à une activité publique en elle-même.

[230] See *e.g. Bombardier Inc., Canadair et Association internationale des machinistes et des travailleurs de l'aérospatiale, loge d'avionnerie de Montréal, section locale 712*, [1996] T.A. 251 (Durand) (exception which confirms the rule).

[231] See Trib. gr. inst. Saint-Étienne, 19 April 1977, *Procureur de la République* v. *Arnould et Meunier*, D. 1978. Jur.123 (listening in on lunch room conversations by means of an intercom) cited in D'Aoust, *supra* note 173 at 44.

[232] See *L'Union des routiers*, *supra* note 207.

[233] See *O'Conner*, *supra* note 64; and *K-Mart Corp. Store No. 7441* v. *Trotti*, 677 S.W.2d 632 (C.A. Tex. 1984), online: LEXIS (GENFED/MEGA), cases based in part on U.S. Const. amend. IV.

b. Time

The work day is divided into moments when an employee is "on-duty" and those when the employee is "off-duty". Increasingly, the distinction between such moments is itself blurred. Pursuant to the terms of the employment contract as supplemented by the terms of an applicable labour code or collective agreement, an employee has time to himself while at work: the lunch hour, coffee breaks, etc. These moments may well be fixed rigidly by contract or applicable statutory provisions, or they may be established informally. Employees often conduct "private affairs", including the use of e-mail or the Internet, during such times. Employers who monitor employee behaviour during such times, even if spent on company property, should accordingly have to justify this intrusion into the private realm.

c. Nature of the Activity

In an era of ever-higher expectations of productivity, the concept of "nine-to-five" is largely disappearing. Working hours can begin very early in the morning and extend well into the evening. In such a context, it becomes implausible to expect that an employee will devote 100% of his time at work to work-related matters. Many employees perform such "personal" tasks as calling the daycare centre, a spouse, or a friend during "working hours". E-mail is used for such purposes in much the same way as is a telephone. E-mail is an efficient, inexpensive manner by which employees communicate not only with each other and with their superiors, but also with extra-professional contacts. Unless informed to the contrary, it seems appropriate that employees have a reasonable expectation that such exchanges are and will remain private.[234]

d. Intensity of the Surveillance

As has been noted on several occasions both in doctrine and jurisprudence,[235] there is a qualitative difference between traditional surveillance and electronic surveillance. While it may be appropriate for an employer to monitor the size of computer files downloaded from the Internet to ensure that the server is not overloaded, for instance, it may not be appropriate for an employer to systematically review the content of all e-mail messages sent by employees.

Conclusion

While Canadian courts have yet to address the question of whether employers have a right to monitor employee e-mail and Internet use (and, if so, under what circumstances), a review of applicable legislation, jurisprudence, and doctrine suggests that employee privacy rights mitigate against the suggestion that employers have an unfettered right to monitor.

---

[234] See *e.g. Weir, supra* note 120.

[235] See *e.g. Duarte, supra* note 27.

Employers have the right to direct and control their employees' work. Moreover, they have the right to expect faithful service from their employees and to protect their proprietary interests, whether they be in respect of confidential information, intellectual property, or, more simply, the need to protect company software against viruses or company hardware (such as the hard-drive on servers) from overuse.

Nevertheless, these rights should be balanced against employees' rights of privacy, both for the sake of the employee and in the interests of a healthy working atmosphere designed to inspire creativity, independence, and productivity. Perhaps the best manner by which to effect an appropriate balancing of countervailing employee and employer rights is to draft and implement an e-mail and Internet use policy and to ensure that employees have both read its terms and have agreed to be bound by them.

The policy should be reasonable. It should set forth terms of use and circumstances of monitoring which are consistent with the goal of protecting both the company and its employees against misuse and liability, whether resulting from harassment, defamation, breach of confidential or proprietary information, or any other inappropriate use. It should make clear that any personal information gathered by means of the implementation of the monitoring policy will be used only to effect the stated purpose.

Employee consent must be clearly obtained. Moreover, a company should not monitor its employees' use of e-mail and the Internet to any greater extent than it has set out clearly in its monitoring policy. Employees consent to this form of monitoring, but no more.

In order to ensure that employees have read and understood a corporate e-mail and Internet policy, such that the consent statement becomes applicable to them, it would be advisable either to have employees sign a written consent form in which they acknowledge having read the policy and consent to abide by its terms, or to develop an introductory computer screen with a message of the following nature: "Use of this e-mail and Internet system implies that the employee has read and agrees to abide by the terms of Company X's E-Mail and Internet Policy" while, at the same time, providing direct on-screen access to the policy itself (*e.g.* "Click here to read Policy").

Monitoring practices should be transparent. Surreptitious monitoring should be avoided, unless based on a reasonable suspicion of wrongdoing or insubordination. Even then, it would be preferable to have established the parametres and the justification for such monitoring in advance with employees' knowledge and consent. Under certain circumstances, in the case of suspected criminal behaviour, for instance, it may be advisable to seek assistance from appropriate authorities.

Employers are rightfully concerned that their investments in information technology tools might be misused by employees. At the same time, respect for employees' sense of well-being and right of privacy, the encouragement of a healthy work atmosphere, and adherence to the law all mitigate against unfettered or surreptitious monitoring of employee e-mail and Internet use.