Employee Privacy: The Need for Comprehensive Protection

Jeremy F. de Beer, University of Ottawa
hat the number will eventually reach 18,000—have launched litigation singly or in groups, or in one case in a mammoth class action suit, to obtain compensation. These actions focus on one or more forms of damage: cultural loss through aggressive assimilation campaigns such as the suppression of Aboriginal languages, physical abuse, and sexual abuse. As of the end of 2002, only a dozen cases had made their way through the courts, although more than 500 had settled out of court, usually in instances where there were prior convictions of residential school staff members. The federal government estimates that resolving all the residential school abuse litigation in the courts will cost more than $2.3 billion and take longer than half a century.

In the process, the litigation would probably bankrupt all the churches or missionary bodies that were involved in residential schooling, two Anglican dioceses having been pushed into or to the brink of bankruptcy and one Oblate Province approaching insolvency by late 2002.

The federal government is poised to try to speed up the process of resolving the residential school suits while staying off the insolvency of the churches. It is negotiating arrangements with the Anglican, Presbyterian, and United Churches to share the cost of settlements reached through a seven-year program to validate and make awards by a system of adjudication that will avoid the adversarial, cumbersome, and costly courts. By this proposed plan, government and churches will share the cost of compensation on a 75:25 basis, with each Church's potential liability capped at a negotiated amount. Litigants who agree to go through this resolution system rather than the courts must agree not to attempt to appeal the results and must forego seeking damages for cultural loss. In other words, under this alternative system, compensation will be available only for physical and/or sexual abuse, and not for loss of language or other forms of assimilation.

Although these proposals are promising, even they will not bring the long and harrowing residential school story to a final close. There are several reasons for this. The Roman Catholic bodies that operated three-fifths of the schools have thus far declined to enter into negotiations for an alternative system on the government's terms. The Saskatchewan law firm that represents more than one-third of all the claimants is reported to be advising its clients not to avail themselves of the adjudicatory system, but stay with litigation in the courts. Finally, many claimants argue that it is cultural loss that most concerns them about the damage done to them by their exposure to residential school. Clearly, even after almost three centuries and a succession of phases, the story of Canada's Native residential schools goes on.

Employee Privacy: The Need for Comprehensive Protection

Jeremy deBeer*

Society has begun to pay more attention to privacy. This is especially true in the context of the employment relationship, where a power imbalance creates a greater need for privacy protection. Although some steps have been taken, Canadian lawmakers have fallen short in their efforts to safeguard the privacy of all employees. Employers are presently protected by a piecemeal scheme of legislative, common law and market-based mechanisms, which leaves a substantial gap in the Canadian privacy framework. In only tenable solution is for each province to enact laws that address privacy in the employment context, using recently enacted federal privacy legislation as a template.

"Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual...the right 'to be let alone...'[Numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the housetops.']**

I. INTRODUCTION

As information plays an increasingly prominent role in people's activities, transactions, and relationships, ownership of and access to it becomes more valuable. The ease with which information can now be collected and disseminated has not only increased this value, but has also heightened awareness of it. Therefore, it is not surprising that we treat the right to control such an asset—our privacy—with the utmost regard.

---

1. B.Comm., LL.B., University of Saskatchewan. I thank Beth Wilson for her insightful comments on an earlier draft of this article and Megan M. Tedford for her assistance with this version.


3. Legal scholars, courts, and legislators often view privacy as a personality right rather than a property right. As such, it is inextricable unlike many tangible "assets." See Charles Morgan, "Employees' Monitoring of Employee Electronic Mail and Internet Use" (1999) 45 McGill L.J. 889 at 885. Although certain elements of privacy may have intragroup worth, other privacy aspects are capable of monetary
Privacy is not an absolute right. There are occasions where the right to prevent intrusion into one's private life must yield to competing interests. The interests at stake in an employment context are unique and, therefore, deserve special consideration. Although some intrusion of employees' privacy may be justifiable, the extent to which encroachment is necessary is debatable.

Judges, arbitrators, legislators, politicians, and other policy makers have not been unmindful of the power imbalance that often exists in the employment relationship, and have previously attempted to balance employees' needs and employees' rights. In general, international agreements establish privacy as a fundamental human right. Where governmental bodies are concerned, the Canadian Charter of Rights and Freedoms\(^3\) can be applied to prevent unjustifiable intrusions. Certain government organizations are subject to the Privacy Act.\(^4\) Recently, Parliament has created the Personal Information Protection and Electronic Documents Act,\(^5\) which addresses employees of federal works, undertakings and businesses, and privacy rights generally. Some provincial legislatures have codified the tort of invasion of privacy, or supplemented privacy protection in other ways. Private sector employees might potentially turn to tort law, which has often been interpreted in light of Charter values, as recourse against intrusive employers. In the context of collective bargaining, unions can consolidate the negotiating power of employees to offset the power imbalance in the employment relationship.

However, there are few mechanisms capable of protecting the privacy of individual private sector employees in the master-servant relationship. Because they lack the bargaining power of unionized workers and the protections afforded to employees in the federally regulated and public sectors, individual private sector employees have little recourse against employers who violate their rights of

---

\(^{3}\) valisation. For example, customer lists or qualitative information about an individual's spending habits might be valuable assets. Indeed, information has been described as a raw material that drives the industry: see Information and Privacy Commissioner/Canada, Privacy: The Key to Electronic Commerce (Ottawa: Information and Privacy Commissioner/Canada, 1998), online: Information and Privacy Commissioner/Canada <http://www.ipc.on.ca/docs/ico-comm.pdf>.


\(^{6}\) S.C. 2000, c. S [PPIPED Act].

\(^{7}\) This article draws a distinction between private and public sector employers. These terms are used in their traditional sense. That is, public sector employees are those employed by the Government of Canada, provincial governments and all government departments or agencies. Private sector employees are those working for non-governmental businesses, in a very broad sense. Employees of federal works, undertakings and businesses are generally included within this private sector, unless indicated otherwise. Independent contractors are not the subject of this article.

---

privacy. Moreover, the few option have significant shortcomings. Unfortunately, the PIPED Act has sector employment relationships provincial context.

The purpose of this article is to employee privacy rights and exp existing therein. I propose that one must fill the gap in the current, pit end, I begin by introducing the protection in general, and in an e then provide a synopsis of the privacy in order to demonstrate: individual, private sector employment provincial legislation, based upon modification, greatly benefit these that provincial legislation must preservation is now safeguarded only by a patchwork of legal protection.

II. DEFINING PRIVACY

A. CONTENT

Many legal scholars have tried to precise definition, yet perhaps provided by Samuel D. Warren and article, "The Right to Privacy."\(^7\) Common law, describe the right to the right to be let alone.\(^8\) Other expression of personal security and as the individual's right to it extent information about him or The Supreme Court of Canada physiology.\(^11\)

Perhaps it is easier not to see privacy, but rather to elaborate U the United States, privacy has been following four distinct rights: (1)
privacy. Moreover, the few options that do exist, such as tort actions, have significant shortcomings that render them ineffective. Unfortunately, the PIPED Act has only limited application to private sector employment relationships, since it does not apply in the provincial context.

The purpose of this article is to explore the legal regime surrounding employee privacy rights and expose the substantial deficiency that exists therein. I propose that comprehensive provincial legislation must fill the gap in the current, piecemeal protection scheme. To that end, I begin by introducing the substance and importance of privacy protection in general, and in an employment context in particular. I then provide a synopsis of the current laws regarding employee privacy in order to demonstrate a significant lack of protection for individual, private sector employees. Next, I show why and how provincial legislation, based upon the PIPED Act could, with slight modification, greatly benefit these employees. Ultimately, I point out that provincial legislation must provide relief to employees whose rights are not safeguarded only by an inconsistent and often ineffective patchwork of legal protection.

II. DEFINING PRIVACY

A. CONTENT

Many legal scholars have tried to capture the essence of privacy in a precise definition, yet perhaps no better explanation exists than that provided by Samuel D. Warren and Louis D. Brandeis in their seminal article, “The Right to Privacy.” The authors, borrowing from the common law, describe the right to privacy with the succinct phrase, “the right to be let alone.” Others have characterized privacy as an expression of personhood defining the individual’s human essence, and as the individual’s right to determine when, how, and to what extent information about him or her is communicated to others. The Supreme Court of Canada has adopted nearly identical phrasing.

Perhaps it is easier not to seek a comprehensive definition of privacy, but rather to elaborate upon the contents of this right. In the United States, privacy has been expressed as encompassing the following four distinct rights: (1) to prevent intrusion into one’s

---

7 See note 1.
8 Ibid.
9 See Ken Gormley, “One Hundred Years of Privacy” (1992) 79 L. Rev. 1335 at 1335.
11 “Privacy may be defined as the right of the individual to determine when, how, and to what extent he or she will release personal information” R. v. Laine, [1990] 1 S.C.R. 30 at 33, 65 D.L.R. (4th) 240.
seclusion or solitude; (2) to control public disclosure of private facts; (3) to prevent publicity that places one in a false light; and (4) to prevent misappropriation of one's personality. The Supreme Court of Canada provided its own analysis of the content of the right to privacy in R. v. Dyment. In that case, La Forest J. adopted the theory of "zones or realms of privacy," which include rights involving territorial or spatial aspects, rights related to the person, and rights that arise in an information context.

Territorial privacy is perhaps the oldest recognized privacy right. Although territorial or spatial rights were historically connected to property rights, and as such, were largely confined to the home, La Forest J. recognized modern realities and confirmed, "what is protected is people, not places." Privacy of the person "transcends the physical and is aimed essentially at protecting the dignity of the human person." Informational privacy has been the most threatened of privacy rights in recent times. In the words of La Forest J.,

"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 persons to whom, and restricted to the purposes for which it is divulged, must be protected."

A "hierarchy of privacy rights" can also be identified. Privacy surrounding bodily intrusions is most significant and must be afforded the highest degree of protection. Personal property is second in order. In a hierarchy of privacy, the employee is afforded the highest degree of protection. Surrupitious surveillance presents itself on the part of the employer, open surveillance affords the employer some benefit to the employee, for example, I

B. CONTEXT

Evolution in society, particularly the brought a greater awareness of and an employment context, there is an employer's monitoring activities. Information and Privacy Commission of workplace privacy in a detailed workplace context expressed are relevant now. That paper identified three key monitoring practices, employee's personal records. According to the report, the qualitatively changed the nature - techniques including visual, telephone and access control systems such as interfaces. Recently, monitoring practices emerged as a primary concern. Today, the supplement employers' knowledge include drugs, genetic, lie detector.

20 American Management Association, "20th Surveillance: Silhouette of Key Finding Association, 2001), online: AMA - ema's, short 2001 pdf. The study notes record and review employee communicative includes monitoring of telephone calls, video surveillance, alarming, this is occurred in 1997 and is a significant data collected represents the American type, indicative of Canadian trends.

21 Information and Privacy Commissioner, Paper (Toronto: Information and Privacy Information and Privacy Committee, supra note 21, Workplace Privacy).

22 Ibid. at 5-9. Some employers have even used an employee's stress test to jobs or to help assess an employee's stress level and li Testor, "The Dynamics between Public, Protection: A Call for Legitimate Privacy.

23 Workplace Privacy, supra note 21 at 8-11.
afforded the highest degree of protection. Intrusions by searches of personal property are second in order of importance. Surveillance cases are a third category in the hierarchy, and include several subcategories. Surrupitious surveillance presents the greatest potential for mischief on the part of the employer, open surveillance may balance employee and employer rights, and benign surveillance can actually be used to benefit the employee, for example, in training exercises.

B. CONTEXT

Evolutions in society, particularly technological developments, have brought a greater awareness of and need for privacy protection. In an employment context, there is evidence of a rapid increase in employers’ monitoring activities. More than a decade ago the Information and Privacy Commissioner of Ontario explored the issue of workplace privacy in a detailed consultation paper, and the concerns expressed are relevant now more than ever.

This paper identified three specific areas of concern: electronic monitoring practices, employee testing practices, and employment records. According to the report, technology “has quantitatively and qualitatively changed the nature of monitoring” by introducing techniques including visual, telephone, and computer-based surveillance, and access control systems such as cardkeys or biotechnological interfaces. Recently, monitoring of Internet and email usage has emerged as a primary concern. Testing procedures are also being used to supplement employers’ knowledge of their employees, and might include drug, genetic, lie detector, or psychological testing.

20 American Management Association, “2000-AMA Survey: Workplace Monitoring & Surveillance: Summary of Key Findings” (New York: American Management Association, 2001), online: AMA <http://www.amanet.org/research/pdfs/ems_short2001.pdf>. The study noted that three-quarters of major U.S. firms record and review employee communications and activities in the workplace. This includes monitoring of telephone calls, Internet and email use, computer files and video surveillance. Alarmingly, this represents double the monitoring that occurred in 1997 and is a significant increase over 1999 figures. Although the data collected represents the American experience, such information is nonetheless indicative of Canadian trends.


22 Ibid. at 3-8. Some employers have even used chair sensors to determine how much an employee is seated in his or her chair, and voice sensors on telephones can assess an employee’s stress level and honesty. See Laura B. Pacius & Clayton Trotter, “The Disparity between Public and Private Sector Employee Privacy Protections: A Call for Legitimate Privacy Rights for Private Sector Workers” (1995) 33 Am. Bus. L.J. 51.

23 Workplace Privacy, supra note 21 at 8-11.
have nothing to do with performance might argue that such information is discussed below. The point here is that employees may be concerned if unwarranted, and often, such concern
This concern may be apparent in
when privacy is, or is perceived to be uncomfortable and invaded.20 Note alert to this concern because of its conditions. Arguably, not only are excessive invasions of privacy, but and compensation claims may also. Even where employees concede employer is relevant, other concern to the accuracy of information collected employer. Difficulties might arise who inaccurate information and that, instance, to subsequent potential or false information may lead to a d individual or to refuse employment compounded where the employee is
Employees might also be concerned is, having voluntarily entrusted an and information about themselves, emp that such information remain sec employees might be interested about medical records, employment histor

2. Employer Interests
Employer interests that might just broken into three broad categories intrusion is necessary to promote of suggest that productivity losses from or shopping using company computer techniques such as keystroke, Intern surveillance, employers might ensue resources. Employers might argue in

Indeed, it is rare that employers will be entirely irrelevant. The challenge is de
See Ford, supra note 20 at 99.
Ford has argued that invasions of priv integrity", ibid. at 100.
But see e.g. Jeffrey Fifer, "Why Spy? To Stage Sounds Like a Smart Way to Keep Surf", Business 2.0 (February 2003).

27
26
25
24

24 See supra note 12 and accompanying text;
25 See generally Morgan, supra note 2.
have nothing to do with performance on the job. Employers, of course, might argue that such information is necessary for a variety of reasons, discussed below.27 The point here is simply that in some circumstances, employees may be concerned that employers’ intrusions are unwarranted, and often, such concerns are well-founded.

This concern may be apparent in the atmosphere of the workplace; when privacy is, or is perceived to be, invaded, employees may feel uncomfortable and insulted.28 Notably, employers are usually more alert to this concern because of its detrimental effect on working conditions. Arguably, not only are creativity and innovation stifled by excessive invasions of privacy, but hidden costs such as absenteeism and compensation claims may also be increased.

Even where employees concede that information sought by an employer is relevant, other concerns may arise. One of these relates to the accuracy of information collected, used or disseminated by an employer. Difficulties might arise where an employer’s records contain inaccurate information and that information is passed on, for instance, to subsequent potential employers seeking a reference. The false information may lead to a decision either to terminate the individual or to refuse employment in the first place. This problem is compounded where the employee is ignorant of the inaccuracy.

Employees might also be concerned about confidentiality. That is, having voluntarily entrusted an employer with potentially sensitive information about themselves, employees should be able to expect that such information remain secret and secure. Understandably, employees might be worried about employers’ handling of their medical records, employment history, or other personal data.

2. Employer Interests

Employer interests that might justify invasions of privacy can be broken into three broad categories. First, employers might argue that privacy is necessary to promote efficiency in the workplace. Some suggest that productivity losses from employees browsing Web sites or shopping using company computers can be substantial.29 Through techniques such as keystroke, Internet or email monitoring, or video surveillance, employers might ensure that employees are not wasting resources. Employers might argue monitoring is necessary to obtain

27 Indeed, it is rare that employers will waste resources seeking information that is entirely irrelevant. The challenge is delineating the relevant from the irrelevant. See Ford, supra note 26 at 99.
28 Ford has argued that invasions of privacy are, in this respect, an “affront to integrity” ibid. at 100.
information and improve production methods or customer service. Alternatively, monitoring might be used merely for training or educational purposes. Sometimes information is necessary for simple administrative tasks, such as payroll or other organizational matters. Employers may require medical information to properly evaluate issues of reasonable accommodation when dealing with matters of disability.

The second justification that employers may cite is based upon vicarious liability for acts or omissions of employees. Also, certain employees can create binding contractual obligations on employers. Since control is arguably dependent on the ability to observe and evaluate employee activities, or to obtain information about honesty and reliability in the first place, some degree of intrusion into employee privacy may be necessary. An individual’s right to privacy might also be constrained by the Extent that information is reasonably necessary to prevent injury to others. For example, alcohol and drug testing of air traffic controllers may be justified by public safety concerns. Employers are entrusted to ensure the safety of other employees in the workplace, and in fact, are often under a statutory or common law duty to do so. For example, monitoring of Internet and email use may be required to avoid liability in harassment suits. Information about medical history might be necessary to guard against the possible spread of disease. Also, employers may be required to ensure that positions of trust and security are not abused, particularly given recent concerns about terrorism.

Finally, employers might cite ownership of property as a reason to violate employee privacy. That is, employers almost invariably own the property used by their employees and thus have a legitimate interest in ensuring that property is not used mischievously. For instance, it is arguable that video surveillance directed at cash tills is required to prevent employee theft. An employer may justify Internet and email monitoring policies on the grounds that the computer system is a company asset. As is evident from the various justifications for Internet and email monitoring in particular, it is not uncommon for employers to cite multiple justifications for their policies and practices.

3. The Power Imbalance

As we can see, in most cases, there is tension between employees’ interests in maintaining their privacy and employers’ interests in obtaining information. Achieving balance is a difficult task because employees are rarely in a position to demand additional job applicants are likely to have additional job offers. These power dynamics may subdue the interests of employees. Thus, employers have virtually unfettered discretion regarding their employees. Further resources to commence and pursue legal actions when violations do occur. For those whose privacy rights attempts, in part, to for these reasons, it is especially in effective and efficient as possible.

III. THE EXISTING LEGAL ORDER

Although each form of protection is capable of fully protecting examination of the legal regime emerging, the scheme of protection of number of employees fall through safeguards for their privacy.

A. INTERNATIONAL PRIVACY

Although a full review of privacy is beyond the scope of this article, conventions and agreements that are recognized as a fundamental human right in documents, including the United Nations Declaration on Human Rights.


31 This discussion is not intended to be privacy protection that exists, but it is not to the employment relationship.


34 This impact can be either direct, through or indirect, in in cases where Canada and directives or initiatives of other governments.

GA Res. 217(U.I), UN GAOR, 52nd sess., 51.

36 19 December 1966, 999 U.N.T.S. 171

37 A/6316.
employees are rarely in a position of equal bargaining power, and are therefore often unable to protect themselves. Employers are more likely to have additional job applicants than prospective employees are likely to have additional job opportunities. Often, employers have little power to negotiate the terms of the employment relationship. Thus, employers have virtually unfettered access to private information regarding their employees. Furthermore, employees often lack the resources to commence and pursue claims against employers, if and when violations do occur. For these reasons, the legal regime surrounding privacy rights attempts, in part, to offset employee vulnerability. Also for these reasons, it is especially important that the legal regime be as effective and efficient as possible.

III. THE EXISTING LEGAL REGIME

Although each form of protection described below has its merits, notice is capable of fully protecting all types of employees. An examination of the legal regime exposes a significant gap in the existing scheme of protection of employee privacy rights. A large number of employees fall through the cracks, and have no adequate safeguards for their privacy.

A. INTERNATIONAL PRIVACY PROTECTION

Although a full review of privacy protection in the international sphere is beyond the scope of this article, there is a variety of treaties, conventions and agreements that affect Canadian law. Privacy is recognized as a fundamental human right by several international documents, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the European Convention on Human Rights.


33 This discussion is not intended to be a thorough analysis of the wide variety of privacy protections that exist, but is merely to address each mechanism's relation to the employment relationship.


35 This impact can be either direct, through treaties to which Canada is a signatory, or indirect, in its cases where Canadian law has been influenced by unintentional directives or initiatives of other governments around the world.


Convention for the Protection of Human Rights and Fundamental Freedoms.\textsuperscript{38} These documents recognize the right to privacy in general terms, and are important in that they clearly establish the value of privacy as a human right. However, they do not contain specific guidelines concerning the nature of the right to privacy or impose specific obligations to ensure privacy protection.

Two instruments have been particularly important to developing international privacy guidelines: the Council of Europe’s 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data\textsuperscript{39} and the Organization for Economic Co-operation and Development’s (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.\textsuperscript{40} The Council of Europe’s Personal Data Protection Convention sets out standards for data management, and is legally binding on those countries that have ratified it. The OECD Guidelines outline several fundamental principles that form the cornerstone of fair information practices for member states, but are not legally binding on Canadian organizations.\textsuperscript{41}

In short, these international instruments establish privacy as an important right, and recognize the need for protection. They are models upon which organizations are encouraged to base their privacy policies, and indeed provide a basis for Canadian legislation. However, international documents themselves do little to actually protect the interests of specific employees, who must therefore turn to domestic laws for protection.

\textsuperscript{38} 4 November 1950, 213 U.N.T.S. 221, art. 6, Eur. T.S. S.
\textsuperscript{41} These principles include collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability. See Barry S. Sookman, Sookman: Computer, Internet and Electronic Commerce Law, 2nd ed. (Scarborough, Ont.: Carswell, 1994) at para. 8.2(b). The Canadian government endorsed the OECD Guidelines in 1984. Although compliance was encouraged, it was not mandatory. In 1998, the European Union Data Protection Directive came into force: EC Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) O.J. 281/3. The Directive requires member countries to provide equivalent data protection standards, which, if not met, would prevent the transfer of data to such countries. The practical result of this was that unless Canada enacted adequate standards, data might not be transferred to this country, leaving Canada at a disadvantage with respect to modern economic realities. See Bruce Phillips, “The Evolution of Canada’s Privacy Laws” (Speaking Notes prepared for the Canadian Bar Association—Ontario Institute 2000, 28 January 2000), online Privacy Commissioner of Canada <http://www.privcom.gc.ca/speech_archive/02.05_e_004128_e.aspx>.

B. THE CANADIAN CHARTER C

Since its introduction in 1982, the privacy rights are protected in Charter, express right of privacy, Canadian right within the provisions of the notwithstanding Clause and Section 7 recognizes that “every and security of the person, and the except in accordance with the prin The Supreme Court of Canada has an right against intrusions under of Game. To determine whether must consider the nature of the relationship between the party and the party claiming its on the information was obtained, it was obtained.\textsuperscript{46}

It may also be important to examine disclosed in evaluating the reaso privacy.\textsuperscript{47} It is clear that s. 8 extends co territorial privacy or privacy of the per privacy.\textsuperscript{48} Therefore, it might be ca from potential intrusions by employee

B. THE CANADIAN CHARTER OF RIGHTS AND FREEDOMS

Since its introduction in 1982, the Charter has transformed the way privacy rights are protected in Canada. Although it contains no express right of privacy, Canadian jurisprudence has implied such a right within the provisions of the Charter, particularly within ss. 7 and 8. Section 7 recognizes that "everyone has the right to life, liberty and security of the person, and the right not to be deprived thereof except in accordance with the principles of fundamental justice." 42 The Supreme Court of Canada has acknowledged that privacy may be an element of liberty and security of the person. 43

Privacy is more specifically protected by s. 8 of the Charter, which guarantees that "everyone has the right to be secure against unreasonable search and seizure." 44 This right has been interpreted as a broad and general right against intrusions where there is a reasonable expectation of privacy. 45 To determine whether there is such an expectation one must consider

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, [and] the manner in which it was obtained. 46

It may also be important to examine the reason why information was disclosed in evaluating the reasonableness of an expectation of privacy. 47

It is clear that s. 8 extends constitutional protection beyond territorial privacy or privacy of the person, and can include informational privacy. 48 Therefore, it might be capable of safeguarding employees from potential intrusions by employers involving personal information,

42 Charter, supra note 3.


44 Supra note 3.

45 Hunter v. Southam, supra note 16.


47 Dagg, supra note 43.

48 In Plant, supra note 46, the alleged violation of privacy related to information possessed by an electric utility concerning household electrical consumption. Hunter v. Southam, supra note 16, dealt with protection for business records. Similarly, Dagg, supra note 43, involved copies of logs with the names, identification numbers and signatures of employees entering and leaving the workplace on weekends.
surreptitious video surveillance\textsuperscript{49} or email monitoring.\textsuperscript{50} However, the \textit{Charter} only applies to actions by the state or its agents.\textsuperscript{51} Thus, it may be applicable, for instance, where there has actually been an invasion by a government agency, or where legislation authorizes a violation of s. 8. It has no direct application in the context of private sector employment relationships.

\textbf{C. THE CRIMINAL CODE}

In some situations, employers who invade employee privacy may be guilty of a criminal offence under the \textit{Criminal Code}.\textsuperscript{52} Sections 183 to 196 relate to the invasion of privacy through electronic means. Perhaps most importantly, s. 184(1) states:

\begin{quote}
Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.\textsuperscript{53}
\end{quote}

The definitions of the terms contained in this section seem to indicate that this provision could be applied in an employment context, with respect to email or telephone monitoring, for example.\textsuperscript{54}

One of the most significant considerations in this context is the reasonable expectation of privacy.\textsuperscript{55} Unless there is such an expectation, the communication might not be described as “private” and thus not included within the ambit of s. 184(1). As discussed below, employers may be able to formulate policies in employees’ reasonable expectation imposing criminal liability is estab\textsuperscript{56} be hard to prove that an employer communication,\textsuperscript{57} or fraudulently or any computer service by means of

\textit{Moreover, with respect to s. 18 at least one of which is relevant for employees. Section 184(2)(a) indic\textsuperscript{58} to a person who has the express or of the communication or of the pr an employer can get employees to ag constitute criminal invasions of pu could obtain express consent to m requiring employees to electronic monitoring policies, each time they an employee continues to perform informed monitoring actually occur Notably, however, consent must be g Furthermore, consent to a policy knowledge that the employer is might not constitute consent.\textsuperscript{59}

Thus, in theory, there may be under the criminal law. Unfortunat\textsuperscript{60} is unlikely to be invoked with resg employee privacy rights.

\textbf{D. THE PERSONAL INFORMATIVE ELECTRONIC DOCUMENTS ACT.\textsuperscript{61}}

Although widespread return of privacy before\textsuperscript{62} international documents z


\textsuperscript{50} See R. \textit{v. Wier} (1998), 213 A.R. 285, [1998] 8 W.W.R. 228, 1998 ABQB 36 (Alta. Q.B.). When police, acting on a tip from the accused’s Internet service provider, searched the contents of an email containing child pornography, there was a violation of the reasonable expectation of privacy, although the evidence collected was ultimately admissible.

\textsuperscript{51} Charter, supra note 3, s. 32(1).

\textsuperscript{52} B.C.S.C. 1985, c. C-46.

\textsuperscript{53} Ibid.

\textsuperscript{54} Section 183 of the Criminal Code defines “intercept” to mean “listen to, record or acquire a communication or acquire the substance, meaning or purport thereof”\textsuperscript{55} ibid. The term “private communication” includes any “oral communication, or any telecommunication, or any communication 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”. ibid.


\textsuperscript{56} See Criminal Code, supra note 52, s. 193 makes it an offence to wilfully make an intercepted private communication.

\textsuperscript{57} See Criminal Code, ibid., s. 14(1)(b) [emphasis added]. Arguably, these provis of employees’ email exist. See Morgan, n


\textsuperscript{59} See Watkiss v. L.M. Berry & Co., 704 E.; intercept the Americans Electronic Co. No. 59-508, 100 Mat. 1808 [G.C.U.]. Alt Morgan notes the striking similarities by Canadian Criminal Code; supra note 2 at 1.

\textsuperscript{60} The Uniform Law Conference of Canada, Criminal Code, supra note 2 at 1.

\textsuperscript{61} See Sikorski, supra note Canada was to introduce data protect
Employees who invade employee privacy may be guilty of an indictable offence "sign" a form, which describes monitoring policies, each time they log onto a company computer. If an employee contemplates to perform certain tasks after they have been informed monitoring actually occurs, consent might even be implied. Notably, however, consent must be given freely and without coercion. Furthermore, consent to a policy of general monitoring or mere knowledge that the employer is capable of monitoring activities might not constitute consent. Therefore, in theory, there may be some protection for employees under the criminal law. Unfortunately, in practice, the Criminal Code is unlikely to be invoked with respect to employer intrusions upon employee privacy rights.

D. THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT

Although widespread reform of privacy legislation had been contemplated before,60 international documents and agreements provided the final

---

60 See Criminal Code, supra note 52, s. 193(1), which, subject to various exceptions, makes it an offence to willfully make known to another person the existence of an intercepted private communication.

61 See Criminal Code, ibid., s. 342(1)(b) and the relevant definitions in s. 342(1-2) [emphasis added]. Arguably, these provisions can be applied to employer monitoring of employees' email use. See Morgan, supra note 2 at 878.


64 The Uniform Law Conference of Canada has been working toward uniformity of legislation across Canada, but suspended its work upon the enactment of Bill C-4 (PIPEDA). See Sokolnik, supra note 41 at para. 8.16, n. 435.1. Prior to that, Canada was to introduce data protection provisions into the Canadian Human
impetus for action in Canada. In response to worldwide demands for privacy and data protection, the PIPED Act was introduced in October 1998 and received Royal Assent on April 13, 2000. It is general, organizations subject to the PIPED Act must obtain consent to collect, use or disclose personal information about an individual. The individual has the right to access that information and challenge its correctness. If an organization wishes to use information for a purpose beyond the limited purpose for which it was obtained, the organization requires the individual’s consent. Information must also be safeguarded by security measures to prevent its misappropriation.

Part 1 of the PIPED Act specifically contemplates application to personal information about employees that is collected, used or disclosed in connection with the operation of a federal, undertaking or business. Federal works, undertakings and businesses are those under the legislative authority of Parliament under s. 92 of the Constitution Act, 1867. Hence, this legislation has the potential to benefit a large number of private sector employees, although only in the federal context.

Conceivably, employees of non-federal works, undertakings or businesses might also be protected by the PIPED Act, since it applies to organizations with respect to personal information that the organization collects, uses or discloses in the course of commercial activities. “Commercial activity” is defined as “any particular transaction, act or conduct or any regular course of conduct that is of a commercial character.” Arguably, employee monitoring or other forms of privacy invasion on the part of an employer is a commercial activity. However, decisions of the courts indicate that a flow of considerer is triggered. Thus, it seems that the employees’ information itself is the or is somehow disclosed outside. Thus, the PIPED Act does not govern in the federal context.

Any remaining ambiguity in the employees’ personal information get constraints. Given the limited scope and commerce, it seems that Parliament to enact laws that purport provincial context. Indeed, this expressly includes only employees of excludes employees of non-federal
other forms of privacy intrusion could be of a commercial character by virtue of the fact that they occur within the scope of business activity. However, decisions of the Privacy Commissioner of Canada indicate that a flow of consideration is required before this clause is triggered. Thus, it seems that the PIPEDA Act would only apply when employees’ information itself is the subject of a commercial transaction, or is somehow disclosed outside of the employment relationship. Thus, the PIPEDA Act does not govern employment matters, other than in the federal context.

Any remaining ambiguity in the potential for this clause to apply to employees’ personal information generally is resolved by constitutional constraints. Given the limited scope of the federal power to regulate trade and commerce, it seems constitutionally impermissible for Parliament to enact laws that purport to govern employees in a provincially provincial context. Indeed, this is the reason that the PIPEDA Act expressly includes only employees of federal works, and by implication, excludes employees of non-federal works. 

67 See PIPEDA Act Case Summary #7: Employee Alleges Non-Commeosial Disclosure by Employer to Investment Firms (28 October 2001), Privacy Commissioner’s Findings under the PIPEDA Act online: Privacy Commissioner of Canada [www.privcom.gc.ca/ltl-dec/dc_0115108.e.asp]. Moreover, until January 1, 2004, the disclosure of information for consideration must occur across borders. After that date, the PIPEDA Act purports to also apply to transactions within a province.


69 Perrin et al., ibid. at 59, explain that ‘employee information, labour relations, and modernization of the employment relationship are within the jurisdiction of the provinces as falling under property and civil rights, and that relationship is not considered as coming within the ‘raising of commercial’ within the meaning of a commercial character in this proposition, the author’s view that Tarasoff Electric Commissions v. Sadle (1985) A.C. 396, [1985] 2 D.L.R. (5th) 657, 69 D.L.R. (4th) 587; and Reference Re Application of Hours of Work Act (British Columbia) to Employers of the Canadian Pacific Railway in Empress Hotel, Victoria City (B.C.) (1949), 1950 A.C. 122 (F.C.); Oil, Chemical and Atomic Workers International Union, Local 60-640 v. Imperial Oil Limited and British Columbia (A.G.), [1963] S.C.R. 386, 41 D.L.R. (2d) 1; and Canada (A.G.) v. Ontario (A.G.) (Unemployment Insurance), 1957 A.C. 355 (F.C.) However, noting that Parliament may regulate employment in federal works, undertakings and business, they
This leaves inadequate protection under the PIPED Act for the employees of non-federal works, undertakings or businesses whose information is collected, used or disclosed by organizations during the course of many day-to-day activities. Thus, although a substantial number of employees are clearly covered by this legislation, many are not.

E. THE PRIVACY ACT AND THE ACCESS TO INFORMATION ACT

The Privacy Act70 governs the collection of personal information by the federal government, including most agencies and some crown corporations. By setting forth a series of rules regarding, among other things, core privacy principles and access to information rights, the Privacy Act establishes standards for the protection of certain types of information.71 Similar legislation has now been enacted in most provinces.72 The Access to Information Act73 ensures that individuals can access information held about them by government institutions. The obligations imposed by these statutes apply to information in general and not specifically to employee privacy. Nevertheless, there is no reason to suspect they could not be applied in an employment context.

However, for employees, the shortcomings of the Privacy Act and the Access to Information Act are twofold. First and most obviously, they only apply with respect to the federal public sector. Second, their scope is limited to information privacy. Protection is not extended to other forms of privacy rights, such as territorial privacy or privacy of the person. Although it is arguable that information obtained from violations of these other privacy rights would be protected, such rights are not expressly protected.

70 supra note 4.
71 For example, information about race, colour, religion, marital status, educational, medical, criminal or employment history and information about an address, fingerprints or blood type might be protected under the Privacy Act: ibid, s. 3.
E. SECTORAL LEGISLATION
Statutes and regulations govern privacy in a variety of industries, including the credit reporting, financial services, and telecommunications industries, and in specific areas such as health and medical records. These statutes, like the Privacy Act and the Access to Information Act, have only a limited capacity to protect employee privacy because they are restricted to certain sectors and do not address the employment relationship specifically. Moreover, even where they do apply, they create unequal treatment among employees of certain sectors vis-à-vis others.

G. PROVINCIAL LEGISLATION
1. Statutory Torts
Four provinces have enacted legislation that establishes a tort of invasion of privacy. In British Columbia, Saskatchewan, Manitoba, and Newfoundland it is a statutory tort to violate, wilfully and without claim of right, the privacy of another person. The claimant’s reasonable expectation of privacy is central to an assessment of liability under these statutes.

Such legislation is of little value to employees for a variety of reasons, which are worth discussing here, although they are equally applicable to a number of other forms of protection under the common law, mentioned below. First, these tort actions were not created to

74 See Consumer Reporting Act, R.S.O. 1990, c. C-33 (Ontario); Credit Reporting Act, R.S.B.C. 1996, c. 81 (British Columbia); The Personal Information Act, S.M. 1971, c. 23 (C.C.S.M. c. P14) (Manitoba); Consumer Reporting Act, R.S.P.L. 1988, c. C-20 (Prince Edward Island); The Credit Reporting Agencies Act, R.S.S. 1978, c. C-44 (Saskatchewan); and Consumer Reporting Agencies Act, S.N. 1977, c. 18 (Newfoundland).


76 See e.g., Telecommunications Act, S.C. 1993, c. 38; and Radiation Protection Act, R.S.C. 1985, c. R-2.2, s. 9(1)(b).

77 Privacy protection of health and medical records is a result of a patchwork of laws, regulations, professional codes of conduct and the common law. See Sookman, supra note 41 at para. 8.10(c).

78 See Privacy Act, R.S.B.C. 1996, c. 375 [Privacy Act (British Columbia)].

79 See The Privacy Act, R.S.S. 1978, c. P-24 [The Privacy Act (Saskatchewan)].

80 See The Privacy Act, R.S.M. 1987, c. P125.

81 See Privacy Act, S.N. 1981, c. 6.

82 See e.g., s. 611 of The Privacy Act (Saskatchewan), supra note 79; and s. 1(2) of the Privacy Act (British Columbia), supra note 78.
apply specifically in the employment context, and hence may not adequately address the unique problems faced by employees. Vulnerable employees, whose rights are most likely to be violated, will often lack the resources to pursue these actions. Any potential remedies are of little benefit without a simple, accessible and economical mechanism for dispute resolution.

Second, even if an employee were able to procure judgment, monetary damages may not be adequate compensation, especially where privacy violations affect an employee's self-worth or dignity. Also, because of their limited application in an employment context, it is unlikely that these actions are a deterrent that will prevent future invasions of employee privacy.

Third, even if an employee had the resources to pursue an action in tort, they would have to meet a considerable burden to prove their expectation of privacy was reasonable, and that their privacy rights outweigh the competing interests of employers. Notably, employers might be able to influence the reasonableness of an employee's expectation of privacy through the policies they unilaterally impose. For example, if an employer uses conspicuous video surveillance techniques, it might be difficult for the employee to argue they reasonably expected that their activities in view of the camera would be private. Similarly, if an employer discloses its Internet and email monitoring policies to employees, it could be unreasonable to expect that Internet and email use would be private. It might be arguable that those activities should be private, but there may not be the requisite reasonable expectation that they would be private. The fact that employees might be able to determine an employees' expectation of privacy further undermines the efficacy of these forms of privacy protection.

2. Quasi-Constitutional Protection in Quebec

The Quebec Charter of human rights and freedoms83 is quasi-constitutional in that it pre-empts other legislation that violates its provisions.84 The Quebec Charter applies to both the private and public sectors, unlike the Canadian Charter.85 Section 5 of the Quebec Charter is important in establishing the right to privacy and guarantees "a right to respect for...private life."86 In addition, there are provisions that protect the peaceful enjoyment of property87 the inviolability of the home88 and the right of non-disclosure of confidential information.89

---

83 R.S.Q., c. C-12 3 [Quebec Charter].
84 Ibid., ss. 52, 55.
85 See Vez-Vez, supra note 43.
86 Supra note 83.
87 Ibid., s. 6.
88 Ibid., s. 7.
89 Ibid., s. 9.
The two leading cases interpreting privacy rights under the Quebec Charter are Godbout90 and Vice-Versa.91 In Godbout, the Supreme Court of Canada said the right to privacy should be interpreted broadly and openly and included choices about where to live, as well as informational privacy. Vice-Versa dealt with the right to privacy in the context of a private sector dispute. In that case, the Supreme Court balanced competing interests and held that an unauthorized photograph published in a magazine constituted an invasion of the plaintiff’s privacy. For the purposes of this article, these cases signify Canadian courts’ willingness to vigorously protect privacy rights.

There is no reason to suspect the Quebec Charter could not be applied in an employment context. However, it was not designed specifically with the employment context in mind, and is therefore subject to many of the same shortcomings as other forms of protection. Fortunately for employees in Quebec, that province has enacted legislation that addresses these problems.

### 3. Other Provincial Initiatives

Quebec must be praised as the only province that has had for some time comprehensive protection for both public and private sector employees. An Act respecting the protection of personal information in the private sector92 creates “particularly rules with respect to personal information relating to other persons which a person collects, holds, uses or communicates to third persons in the course of carrying on an enterprise.”93 To date, several provinces have begun to take steps to implement their own comprehensive legislation, but neither in Quebec, no adequate laws yet exist.

However, at least two other provinces appear poised to act.94 According to a consultation paper prepared by British Columbia’s Ministry of Management Services Corporate Privacy and Information Access Branch, coverage of all employees’ information in British Columbia is a priority.95 Having recognized the deficiencies in the PIPED Act and the benefits of provincial legislation tailored to that province, legislation may take effect before the end of 2003. Likewise,

---

90 supra note 43.
91 supra note 43.
92 R.S.Q., c. P-39.1 [Quebec Personal Information Protection Act].
93 ibid., A. 1.
Alberta has introduced its own legislation, in order to avoid the application of the PIPED Act in that province as of January 1, 2004. 96

Among the most interesting developments in the provincial context has been in the province of Ontario. Although comprehensive provincial privacy legislation was developed and passed for introduction before the end of 2002, the Ontario government failed to follow through with its plans. In an open letter to the Premier, Ontario’s Privacy Commissioner expressed deep disappointment over the failure to take effect. 97 Indeed, the government’s inaction has received considerable media attention. 98 As it now stands, it seems highly unlikely that Ontario will soon enact comprehensive legislation.

Other provinces, including Saskatchewan, have adopted a “wait-and-see” approach to this issue. The policy seems to be to allow the PIPED Act to take effect in the provincial context and determine at that time whether there is a need for additional privacy protection. As I have demonstrated above, and will continue to explain below, the PIPED Act does not, and cannot apply to employees in a provincial context. Hence, the passive approach taken by many provinces is simply inadequate for a large number of employees.

H. PROTECTION UNDER THE COMMON LAW

1. Common Law Actions

As mentioned above, some provinces have made invasion of privacy a statutory tort. In other provinces, there are indications that such a tort exists at common law. Historically, there was no common law tort of invasion of privacy in Canada, 99 although some courts have chosen not to dismiss claims framed as such. 100 Presently, it appears


97 Ann Cavoukian, Information and Privacy Commissioner/Ontario, to the Hon. Ernie Eves, Premier and President of the Executive Council and Minister of Intergovernmental Affairs, Commissioner’s Letter to the Premier Regarding the Failure to Introduce Legislation (16 December 2002), online: Information and Privacy Commissioner/Ontario <http://www.ipc.on.ca/> (select “Publications and Presentations,” “Special Reports and Submissions.”)


as if there may be such a cause of

Sec 548. v. G101 the Court expressed right to privacy and held that on the

an invasion of privacy and, dep.

of defendant’s counsel that n

plaintiff must be given some r

defendant has in this case done.

The recent application of Charter val

that these tort actions will continue

privacy rights, although a commit

universally accepted. 102

Canadian courts have protected

scope of a variety of established torts.

defamation, and injurious falsehood, breach of confidence, and libel,

agreed employee could potential

Unfortunately, the existence of these
to many employees. In the t

have no access to statutory tort

resources to pursue a common law

also arise regarding the adequacy of

ability of the employer to influence

2. Charter Values

Although the Canadian Charter has disputes, courts have endorsed the provision. Specifically, in Retail, Wholesale and I. v. Delphi Delivery Ltd. 103 the Supreme Court should be developed in a man

Charter values. 102 The application of

a distinct issue from the quest

ought to apply and develop pra

101 [1981], 34 O.R. (2d) 317, 19 C.C.I. T. 37 (Ont.)

102 At 322.

103 See eg. Re Canadian Timken Ltd. and En (Machin Griswold) (2001), 99 L.A. C. (4th)
A detailed discussion of the basis for past


Sokolov, supra note 41 at para. 8.8(b)

as if there may be such a cause of action, at least in Ontario. In Saucier v. Orr,101 the Court expressly recognized the common law right to privacy and held that on the facts there was an invasion of privacy and, despite the very able argument of defendant's counsel that no such action exists...the plaintiff must be given some right of recovery for what the defendant has in this case done.102

The recent application of Charter values to the common law suggests that these tort actions will continue to evolve in favour of protecting privacy rights, although a common law right of privacy is not universally accepted.103

Canadian courts have protected privacy rights by expanding the scope of a variety of established torts.104 Trespass, nuisance, negligence, defamation and injurious falsehood, misappropriation of personality, breach of confidence, and fiduciary duty are all grounds upon which an aggrieved employee could potentially have a tort action.105

Unfortunately, the existence of these causes of action is of limited benefit to many employees. In the same way that many employees have no access to statutory tort remedies, such workers often lack the resources to pursue a common law tort action. The same concerns also arise regarding the adequacy of monetary damages, and the ability of the employer to influence the expectation of privacy.

2. Charter Values

Although the Canadian Charter has no direct application to private disputes, courts have endorsed the possibility of its indirect application. Specifically, in Retail, Wholesale and Department Store Union, Local 580 v. Dolphin Delivery Ltd.106 the Supreme Court held that the common law should be developed in a manner consistent with fundamental Charter values.107 The application of the Charter itself was a distinct issue from the question whether the judiciary ought to apply and develop principles of the common law.

102 Ibid. at 322.
103 See e.g. Re Canadian Titan Ltd. and United Steelworkers of America, Local 4006 (Martha Giovannini) (2001), 98 L.A.C. (4th) 129 (Welling, Ont.).
105 Sookman, supra note 41 at para. 88(b).
107 Ibid.
in a manner consistent with the fundamental values enshrined in the Constitution. In this sense, then, the Charter is far from irrelevant to private litigants.108

This does not mean that all common law disputes ought to be addressed with the Charter in mind.109 Furthermore, the application of Charter values to the common law is not identical to the application of the Charter itself with respect to actions of the state.110 Nevertheless, Charter values have been utilized to protect employee privacy in a number of situations, particularly in labour arbitration hearings.

Perhaps the most significant of these was Re Domain Forest Products Ltd., New Westminster Division and International Woodworkers, Local 1-357.111 The arbitrator used Charter values, specifically those values inherent in s. 8, to balance the right of the employer to investigate a potential abuse of sick leave and the right of the griever to be left alone. He drew a parallel between the powerlessness of an employee to intrusion by the state, as in Hunter v. Southam,112 and the vulnerability of employees vis-à-vis employers.113 Therefore, electronic surveillance could only be justified by an application of the reasonableness standard enunciated in Hunter v. Southam.114 This standard was evaluated by enquiring into the reasonableness of the request for surveillance, the reasonableness of the surveillance methods used, and availability of less intrusive alternatives. In addressing these issues, the arbitrator found that the surveillance was not reasonable and refused to admit videotape and voice evidence into the hearing.

The same test has been applied in other arbitral jurisprudence, although a less onerous standard of reasonableness was used to justify

108 Ibid. at 402.
109 In bulk Ltd v. Church of Scientology of Toronto, [1995] 2 S.C.R. 1138 at para. 95, 126 D.L.R. (4th) 129 [Hill], the majority of the Supreme Court of Canada held that the Charter only applies to private parties to the extent that the common law is found to be inconsistent with Charter values.
110 The balancing of values under the common law should be more flexible than under s. 1 analysis. In addition, the issue of proof is reversed and put upon the party alleging an inconsistency with Charter values: ibid. at para. 98.
112 Supra note 16.
113 Diba Majoub, "Employee Privacy: A Critical Examination of the Domain Decision" (1998) 4 Appeal 73 at 74, Majoub argues that, although the test was appropriate, the arbitrator's standards that the employer was required to meet to justify the intrusion were unnecessarily high, contending that the Domain decision is inconsistent with other arbitral, Privacy Act, and Charter jurisprudence.
114 Domain, supra note 111 at 279.

116 In Re Liberal Ontario Brewers (Toronto Bottlers Union), Local 310 (Interim Award) [1991] G.J. Brandt found that Deloiton (Deloiton), an employer, could apply Charter values reasoning to Domain and other limitation cases "useful in determining how to meet employer interests."
117 See Morgan, supra note 2 at 895.
118 See, e.g., Re Toronto Transit Commission 69 (Royal Glenora) (1999), 88 L.A.C. (4th) note 103; Re Wood Buffalo (Bamfield) Local 1369 (Begg (Glenora) [2001], 98 Tarimachinery and Allied Products and United Steelworkers of Canada (Catfeds) 256; Re Toronto Transit Commission and (Fallon Glenora) (1999), 79 L.A.C. (4th) Association of Machinists and Aerospace C.L.A.D.L. No. 564 (Q1).
mind, with the fundamental values Constitution... In this sense, then, the
irrelevant to private litigants. 108

that all common law disputes ought to be
in mind. 109 Furthermore, the application
common law is not identical to the application
with respect to actions of the state 130
due to protect employees
situations, particularly in labour arbitration

of significance was the Re Dominion Forest Products
Division and International Woodworkers, Local
rised Charter values, specifically those values
since the right of the employer to investigate
leave and the right of the grievor to be
parallel to the powerlessness of an
by the state, as in Hunter v. Southam, 112 and
employees vis-a-vis employers. 115 Therefore,
could only be justified by an application of
shod鸾at in Hunter v. Southam. 114 This
by enquiring into the reasonableness of the
the reasonableness of the surveillance
validity of less intrusive alternatives. In
the arbitrator found that the surveillance was
admit videotape and video voice evidence
been applied in other arbitral jurisprudence,
standard of reasonableness was used to justify

the majority of the Supreme Court of Canada held that
private parties to the extent that the common law is
with Charter values.

under the common law should be more flexible than
addition, the onus of proof is reversed and put upon the
wrong with Charter values, ibid. at para. 98.
In L.A.C. (4th) 275-Victoria, B.C.) (Award) (summarized
cited to L.A.C.).

Privacy: A Critical Exemplification of the Doman Decision
116 Moffat argues that, although the test was appropriate,
a that the employer was required to move to justify the
highly high, contradicting that the Doman decision is
against, Privacy Act, and Charter jurisprudence.

115 See e.g. Re Steet Industrial Products and Teamsters Union, Local 213 (Sadda Grievance)

116 In Re Labatt Ontario Beverages (Class action) and Breweries, Gastrical & Professional
Workers Union, Local 304 (Gastrib v Gagnon) (1994), 42 L.A.C. (4th) 353 (Ont.), arbitrator
G.J. Brandt found that Defelice v Defelice, supra note 106, held that the judiciary, but
not arbitrators, can apply Charter values. The arbitrator refused to accept the
reasoning in Doman and other similar cases in this respect, but nevertheless found
them useful in determining how to strike a balance between employer and
employee interests.

117 See Morgan, infra note 2 at 101.
118 See e.g. Re Toronto Transit Commission and Amalgamated Transit Union, Local 113
(Ryall Grievance) (1999), 88 L.A.C. (4th) 109 (Ont.); Canadian Timken Ltd., supra
note 103; Re West Buffalo (Marine quality off and Canadian Union of Public Employees,
Local 1503 (Roy Grievance) (2001), 98 L.A.C. (4th) 440 (Que.); Re Goodrich Turbomachinery Products and United Steelworkers of America, Local 4970 (Dunwill Grievance) (2002), 103 L.A.C. (4th) 382 (Marquette, Ont.); Re Kollmeyer-Clark Inc. and
Association of Machinists and Aerospace Workers (Andersen Grievance), (1999)
C.L.A.D. No. 549 (Q.).

an employee's invasion of employee privacy. 115 Notably, the application
of Charter values by arbitrators is not universally accepted as
appropriate. 114 However, there does seem to be a consensus that
arbitrators should balance employee and employer interests with
Charter values in mind. 117

In sum, Charter values may be helpful to employers who wish to
protect their privacy. However, a survey of the case law in this area
quickly reveals that these principles are applied almost exclusively in
the unionized sector, where established grievance procedures exist.
Rarely, if ever, have Charter values been invoked with respect to an
individual employment privacy dispute. In the absence of an
accessible mechanism whereby employees can pursue a grievance through
arbitration or a similar process, it is extremely difficult to procure a
remedy for an invasion of privacy. Moreover, when the issue does
arise, it is only when assessing the admissibility of evidence after an
incident has already occurred, which may or may not deter future
violations. 118 Indeed this is evidence that the shortcomings of this
form of protection are similar to those described above with respect
to common law and statutory tort actions. Hence, Charter values do
not truly protect the privacy rights of all types of employees.

I. MARKET-BASED PRIVACY PROTECTION

As the foregoing discussion indicates, one of the most important
ways in which employees can overcome their vulnerability,
and protect their privacy, is through the collective bargaining process.

108 See supra note 2 at 86.
109 See supra note 155 at 69.
110 See supra note 7 at 69.
111 See supra note 16 at 70.
Most individual employees are not in a position to contest an employer's assertion of the right to invade an employee's privacy. However, in combination, a large group of employees pose a substantial threat to the employer and are capable of influencing management policies through collective agreements. Thus, if there has been an invasion of privacy, the grievance procedures that exist in a collective bargaining context provide the much-needed access to adequate remedial mechanisms. Moreover, invasions of privacy can often be prevented in the first instance. In these ways, employee privacy rights in a unionized environment are protected significantly more than in a non-unionized workplace.

No unique formal legal mechanisms to protect privacy, statutory, common law or otherwise, apply strictly to unionized workers. However, through unionization, employees can more easily avail themselves of the protections afforded by the legal regime discussed above. Obviously, this mechanism is not a solution to any of the problems of the non-unionized workforce.

2. Independent Bargaining

Although regulation of employee privacy through constitutional, legislative, or common law protection may seem prudent, some might argue against government, judicial or administrative intervention into private employment relationships. Alternatively, market efficiencies can be used to extrapolate the boundaries of privacy in the workplace by allowing employees to determine how much their privacy is worth. If employees are rational actors who seek to maximize their happiness, they will select their ideal mixture of wages and working conditions. If an employer seeks to invade an employee's privacy, that employee will demand higher wages, or other benefits, in return. If the employee's privacy rights are respected, the employer will be

119 Notably, in most invasion of privacy cases, the collective agreement provides little or no direct assistance. See C.L. (Kit) Rigg, "The Right to Privacy in Employment: An Arbitrator's Viewpoint" in William Kaplan, Jeffrey Sack & Morley Gunderson, eds., supra note 26, 83 at 85. However, a practice of conducting searches or inspections, for instance, might be considered an example of a policy or rule and thus, is usually dealt with under the "management rights" portion of the agreement. Thus, the reasonableness of the search would be a primary consideration in determining whether a violation of employee privacy had occurred. See Beth Rihon, "Search and Surveillance in the Workplace: An Arbitrator's Perspective" in William Kaplan, Jeffrey Sack & Morley Gunderson, eds., Labour Arbitration Handbook, 1992 (Toronto: Butterworths, 1992) 143. The point here is that, in one way or another, the collective agreement plays a role in determining the scope of employee privacy rights. Such is not the case in individual employment contracts. Without a collective agreement, these rights are left to be determined under an individual contract, the terms of which the employee typically has little influence over.

120 See John Edward Davidson, "Revolving and Employee Privacy" (1997/98 8 Geo.

121 Davidson proposes an interesting idea. The author advocates a reduction in the which would essentially limit employers'. It supposedly follows that employees has of a right to violate employee privacy. So argument ignores the various other legal interests of which employees.
Employee Privacy: The Need for Comprehensive Protection

able to pay lower wages. Ideally, the parties will bargain until the marginal utility of increasing privacy intrusion, through monitoring, for example, equals the marginal cost of providing additional compensation. In effect, the employer will buy the right to invade the employee's privacy.120

Unfortunately, employees will still be inadequately protected under this theory. First, the above model presumes that employees are generally able to bargain for higher wages or benefits in exchange for lesser privacy protection. In fact, because employers and individual employees are usually not in positions of equal bargaining power, that is not the case. Second, it is questionable whether regard for an employee's privacy is capable of commoditization in the way this theory might suggest. Furthermore, such analysis fails to consider the effect of surreptitious invasions by employers. Surely, employees cannot bargain with respect to invasions that they are unaware of. Thus, some form of intervention is necessary to safeguard employee privacy.121

A SUMMARY OF EXISTING PRIVACY PROTECTIONS

International treaties and conventions establish the importance of privacy as a human right, and some create guidelines for fair information practices, but these documents provide no practical protection for employee privacy. Constitutional privacy protection under the Charter might protect employees, but only with respect to government actions. The Criminal Code only protects informational privacy, contains many exceptions, and likely would rarely be used in an employment context. The PIPED Act has limited application with respect to employers of non-federal works. Deficiencies also exist with respect to the Privacy Act and the Access to Information Act. Only a handful of provinces, of which Saskatchewan is not one, have expressed a willingness to address this problem with comprehensive provincial legislation. The Charter might be indirectly relevant through the application of Charter values to common law tort actions and to labour arbitration decisions. However, from a practical perspective, these are of little value to non-unionized employees who lack the resources to exploit these safeguards. Non-unionized workers cannot be left on their own to bargain for privacy rights.


121 Davidson proposes an interesting solution in lieu of an all-or-nothing approach. The author advocates a reduction in the use of the expansive superior doctrine, which would essentially limit employers' vicarious liability for employee indiscretions. It supposedly follows that employees would therefore have less incentive, or less of a right to violate employee privacy. See generally Davidson, ibid. However, this argument ignores the various other legitimate reasons (discussed in Part II.C.2., Employer Interests) for which employers might invade employee privacy.
sum, upon examination of the legal regime surrounding employee privacy, the need for comprehensive protection is readily apparent.

IV. FILLING THE GAP

Having identified a gap in employee privacy protection, the crucial question that follows is which of the mechanisms identified above has the greatest potential to serve as a template for reform. Some, such as international instruments, the Constitution, and the Criminal Code, do not represent viable alternatives for obvious reasons. Others, such as statutory or common law tort actions, are appealing but lack the mechanisms necessary to ensure accessibility by employees. Some form of legislative scheme is therefore necessary to create such a mechanism for all employees. Given the constitutional constraints that preclude the application of federal legislation to employees within the provinces, amending the PIPED Act to specifically encompass all employees is not an option either.

However, this does not mean the PIPED Act cannot somehow benefit employees. The power of this legislation lies in its potential to significantly influence the activities of the provinces. Indeed, if a province enacts substantially similar legislation, the PIPED Act ceases to apply in that province. Thus, the PIPED Act sets minimum requirements and encourages provinces to meet or exceed those standards.122

Provincial legislators can and should look to this legislation as a template, which can be slightly modified in order to apply to all employees. Unfortunately, only British Columbia and Alberta have taken advantage of this opportunity, although Quebec must be commended as the leader in this regard for nearly a decade. Other provinces, including Saskatchewan, must follow suit.

Recently, the Privacy Commissioner of Canada has given the two leading provinces, Alberta and British Columbia, reason to hesitate in their initiatives. In letters to the official responsible for the legislation in each respective province, the Commissioner suggests that the provincial bills,123 in their current form, are deficient.124 As such, in


h is report to Parliament, the Commissioner did not recommend that the Government of Canada recognize the laws as substantially similar to the PIPED Act. 125

The Commissioner suggests that both pieces of legislation lack, in part, sufficient protection for privacy rights in employment. This is a curious criticism, given that the PIPED Act has no application to employees within the provinces. Thus, whatever protection these proposed laws contain, it is arguably better than the status quo. The letters note that the PIPED Act, unlike the proposed provincial laws, makes no distinction between information in the employment context and in other contexts. As this paper shows, however, there are sustainable reasons to draw certain distinctions. Thus, provinces should retain some flexibility when balancing employers’ rights, bearing in mind the ultimate goal of improving on the existing employment privacy framework.

Provinces should not be discouraged, therefore, from proceeding. Provincial laws could have effect in the employment context, despite the possibility that they might not be recognized as substantially similar, and consequently, might not entirely pre-empt the PIPED Act. As the PIPED Act does not apply to employee privacy within the provinces, provincial laws can at least supplement the federal legislation in this respect.

This is not to say, however, that provinces should not be encouraged to strive for high standards of protection; they should. The discussion below explains more particularly the ways in which employees and employers could benefit from the introduction of a cognate law in the provincial context.

A. THE FEATURES AND MERITS OF COMPREHENSIVE PRIVACY LEGISLATION

1. Phase-in Approach

The PIPED Act was designed to take effect in three stages. The Act that organizations have the opportunity to evaluate their privacy practices and formulate a strategy to meet its requirements before a law takes full effect is one of its most attractive features. Organizations cannot, nor should they be expected to, alter their ways immediately. Not only does the phase-in application allow organizations to mindfully implement responsible practices, but it also promotes advance voluntary

125 See Privacy Commissioner’s Report to Parliament (2003), supra note 122.

- **Employee Privacy: The Need for Comprehensive Protection**

compliance. This approach is consistent with Canada’s historical strategy of encouraging self-regulation of privacy practices, yet at the same time, it does eventually impose positive obligations upon those who refuse to comply.

2. An Expansive Definition of "Personal Information"

The PIPED Act defines “personal information” as any factual or subjective information, recorded or not, about an identifiable individual. Personal information does not have to be private, confidential, sensitive, or even significant to be protected. Notably, the definition expressly excludes the name, title, business address or telephone number of an employee. However, information about an employer’s age, income, race of blood type, or opinions, evaluations, comments, disciplinary records, credit records, medical records, and other such files would be encompassed within this definition. The terminology used in s. 2 would seem to capture almost anything. Surveillance tapes, drug test results, information collected from Internet and email monitoring and even standard administrative data could be regulated.

The only significant limitation is that the information must pertain to an identifiable individual. Therefore, aggregated data could be excluded from the definition of personal information. Presumably, there can be no breach of an individual’s privacy if no ascertainable individual is involved. In this way, competing interests are carefully balanced in that organizations are permitted to collect and analyze data, albeit only to the extent that such data does not identify particular persons. Thus, organizations are conceded some leeway with respect to invasions of privacy.

The breadth of Information that might be encompassed within such a definition recognizes the variety of privacy rights that exist. Because personal information can be factual or subjective and recorded or not, informational privacy is expanded to acknowledge territorial privacy and privacy of the person. Necessity, invasions of privacy with respect to these latter categories will yield, or somehow involve "information" that is regulated by the Act. These internal balancing mechanisms are desirable features that any provincial legislation should share.

3. Core Privacy Principles

Organizations must follow a code for the protection of personal information. Section 5 of the PIPED Act mandates that every organization must comply with schedule 1 to the Act. The following how each of these principles address and/or employer concerns discussed

a. Be Accountable

An organization must be responsible for its control, including information in its custody and control, and designate an individual who is accountable for its activities. The Act directs their inquiries or concerns, at personal information is protected. For all others, as it is internally privacy for employees.

b. Identify the Purpose

Organizations must identify, document the reasons for collecting personal information. If a new purpose is then again. This might mean employees how surveillance or monitoring act certain information, for instance on of them. Importantly, this principle of employment concerns about the right.

c. Obtain Consent

The individual must consent to the both at the time of collection and Notably, consent should never be or should be voluntarily obtained. The Act favors express consent to the organization. The consent requires control over their privacy. This fundamental shortcomings of other employer to directly influence employee privacy. Moreover, respect for the can a more harmonious, cooperative an therefore will likely benefit both

125 supra note 5, ss. 2(1).
126 ibid.
127 Businesses, consumers, academics, and government agencies developed the code under the auspices of the Canadian Standards Association (CSA). See Privacy

Responsibilities Guideline, supra note 67. The Personal Information (Organizational Code in turn based upon the OECD Guidelines, ¶1 para. 8 (1)).
organization must comply with these obligations, contained in Schedule 1 to the Act. The following overview touches briefly upon how each of these principles addresses one or more of the employee and/or employer concerns discussed at the outset of this article.129

a. Be Accountable
An organization must be responsible for personal information under its control, including information transferred or entrusted to a third party, and designate an individual to ensure compliance with the requirements of the Act. Employees could therefore know where to direct their enquiries or concerns, and could be confident that their personal information is protected. This principle serves as the basis for all others, as it instills privacy protection as a significant priority for employers.

b. Identify the Purpose
Organizations must identify, document, and inform the individual of the reasons for collecting personal information before or at the time of collection. If a new purpose is identified, consent must be obtained again. This might mean employees would have the right to know how surveillance or monitoring activities are being used, and why certain information, for instance on an application form, is requested of them. Importantly, this principle ensures that employers address employees' concerns about the relevance of the information sought.

c. Obtain Consent
The individual must consent to the collection in a meaningful way, both at the time of collection and when a new use is identified. Notably, consent should never be obtained by deceptive means and should be voluntarily obtained. Although consent can be implied, the Act favours express consent to protect both the individual and the organization. The consent requirements give employees significant control over their privacy. This principle remedies one of the fundamental shortcomings of other schemes: the ability of the employer to directly influence employees' reasonable expectation of privacy. Moreover, respect for the consent requirements will result in a more harmonious, cooperative and productive environment, and therefore will likely benefit both employers and employees.

129 For a detailed discussion of these principles, see Perre, supra note 68.
d. Limit Collection
Organizations cannot collect information indiscriminately. If employers respect this principle, employees might no longer be subject to, for example, wholesale video surveillance throughout the workplace, or undisturbing Internet and email monitoring. Again, this might alleviate employees' concerns about the relevance of the information sought by an employer.

e. Limit Use, Disclosure and Retention
Personal information can only be used for those purposes to which the individual consents, and guidelines and procedures should ensure it is destroyed when no longer needed. This might provide additional confidence to employees that employers are not unnecessarily using or retaining information. It also reduces the risk that information will be inadvertently lost or misused by an employer.

f. Be Accurate
Personal information must be kept as complete, accurate and up-to-date as necessary. In combination with several of the other principles, this might address employees' concern that employers possess or disclose inaccurate information about them.

g. Use Appropriate Safeguards
Organizations must prevent the loss, theft, modification or other misappropriation of personal information. This might include protecting employee records with locked cabinets, computer passwords or security clearance measures. This also reduces the risk of loss, theft or misuse of employees' personal information.

h. Be Open
Customers, clients and employees should be informed that an organization has policies and practices regarding the management of personal information. For employees, potential benefits might include the ability to acquire information about their privacy rights in the workplace without unreasonable effort. This also goes a long way toward building a comfortable working environment.

i. Give Individuals Access
Individuals must be informed if an organization has personal information about them, and have the right to request that organizations explain it and how information is used or disclosed. This principle might allow employees to ensure as to an employer's intentions to demote or dismiss them, given the broad definition of "personal information."
1. Challenging Compliance
All principles are intended to be enforceable through a combination of formal redress mechanisms and self-regulation. To this end, organizations must establish procedures to respond to privacy complaints. This last element has the effect of addressing one of the most significant shortcomings of other forms of privacy protection—remedial access. In this respect, employers would have easily available recourse through the organization itself, at least to initiate a complaint or inquiry.

2. Access to Remedial Actions
In addition to the remedial mechanisms that organizations themselves must provide under the last principle, there are several other procedures through which privacy rights are enforced. Arguably, these procedures are among the most auspicious features of the PIPED Act, and an important component of any provincial laws built upon this model.

First of all, provincial legislation should contain "whistleblower" protection that guarantees a complainant’s identity can be kept confidential, except as in the PIPED Act.120 Moreover, employees of an organization that contravenes the legislation must be protected from dismissal, suspension, demotion, harassment or other disadvantage if they report the violation to the Commissioner.131 Such protection can only promote the role of the Privacy Commissioner, who is an essential element of this scheme.

a. The Privacy Commissioner
The Privacy Commissioner of Canada132 plays the role of independent ombudsman charged with the task of investigating complaints under the Privacy Act and the PIPED Act. Branches of the Office of the Privacy Commissioner also advise Parliament, conduct research and educate the public about privacy. One of the Privacy Commissioner’s primary tasks is to receive complaints by individuals whose rights might have been violated, and to investigate those complaints if they appear reasonable.133

This is an extremely convenient and accessible method for employees to voice concerns where their privacy rights are being ignored or jeopardized. In this way, employees have access to a unique dispute resolution mechanism, which they would not have if left to pursue tort actions, for example. Moreover, the Privacy Commissioner

130 See supra note 5, s. 27.
131 Ibid., s. 27(11).
132 See generally the Privacy Commissioner of Canada website, online: <http://www.privcom.gc.ca>.
133 PIPED Act, supra note 5, s. 12; The Commissioner has the power to summon the appearance of persons and compel them to give evidence. The Commissioner is also given extensive investigatory powers to enforce the Act. Ibid., s. 12.
does not discriminate between unionized and non-unionized employees; all employees have access to the available procedures. As is consistent with Canada's preference for voluntary compliance, the Commissioner may attempt to resolve complaints through dispute resolution mechanisms such as mediation and conciliation.134 If this is insufficient, the Commissioner has the authority to make a report to the Attorney General and to disclose the practices of an organization to the public. These non-traditional enforcement mechanisms strongly encourage organizations to adopt the Commissioner's recommendations out of a fear of negative publicity. In this way, they are possibly more effective than typical court proceedings.

b. Federal Court of Canada Proceedings
An individual may apply to the Federal Court of Canada for a hearing regarding their allegations.135 Importantly, in the case where an individual cannot or does not do so, the Commissioner can apply for a hearing on the individual's behalf.136 The Court has the power to order an organization to (a) alter its practices to comply with the Act; (b) publish notice of action taken to correct its practices; and/or (c) award damages to the complainant, including compensation for humiliation suffered.137 In combination, the aforementioned remedies go far to address many employees' inability to enforce their privacy rights through existing mechanisms. Access to some form of judicial intervention should, therefore, also form part of a provincial scheme.

Recently, however, questions have emerged regarding the jurisdiction of the Federal Court to review the Commissioner's decisions. In *L'Éveauer c. Aéroports de Montréal*,138 the Federal Court Trial Division held that a labour arbitration panel under the Canada Labour Code, not the Court, was the appropriate forum to resolve the parties' dispute. Also, a British Columbia court recently held that the Privacy Commissioner does not have the power to commence a suit by filing a statement of claim.139 Provincial lawmakers would be wise to consider these issues carefully in order to avoid such ambiguity.

5. Exceptions
There are several important exceptions contained within the *PIPED Act*, which serve to balance the competing interests of employers and employees. First, there is a limitation that personal information must be about an *identifiable* individual, and there are exemptions for

---

134 Ibid., s. 12(2).
135 Ibid., s. 14. See *Englander v. Telus Communications*, 2003 FCT 705.
136 *PIPED Act*, supra note 3, s. 15.
137 Ibid., s. 16.

domestic, artistic, journalistic or literary that, subject to some limitations, access refused where such access would reveal i Section 7 sets forth circumstances in which information may be collected used or disclosed. Specifically, this is the case when th the interests of the individual and con obtained, such as during a medical e context, the other situation where cc employers. Section 7(1)(b) eliminates the collection of information where the availability or accuracy of such information is for purposes relating to agreement or contravention of law. Th employee to monitor an employee and the employee is reasonably suspect e employment contract.

6. The *PIPED Act* in Operation

The Privacy Commissioner has area regarding allegations by employees of b business of privacy violations. If have involved, for example, airport telecommunications companies. In
Canada’s preference for voluntary compliance, attempt to resolve complaints through dispute such as mediation and conciliation. If this commissioner has the authority to make a report and to disclose the practices of an organization non-traditional enforcement mechanisms to adopt the Commissioner’s for the protection of a privacy, in this way, effective than typical court proceedings. Canada Proceedings

To the Federal Court of Canada for a hearing. 

Importantly, in the case where an action taken to correct its practices; and/or the complainant, including compensation for In combination, the aforesaid remedies to employees’ inability to enforce their privacy mechanisms. Access to some form of judicial structure also form part of a provincial scheme. Many questions have emerged regarding the federal Court to review the Commissioner's case. 

Airports de Montreal The Federal Court at a labour arbitration panel under the Canada Court, was the appropriate forum to resolve the British Columbia court recently held that the does not have the power to commence a suit

does not. The Provincial lawmakers would be wise to carefully in order to avoid such ambiguity. 

2003 FCT 705. 15. 15.


domestic, artistic, journalistic or literary purposes. Section 9 explains that, subject to some limitations, access to personal information may be collected used or disclosed without the individual's consent. Specifically, this is the case when the collection is clearly in the interests of the individual and consent cannot be realistically obtained, such as during a medical emergency. In an employment context, the other situation where consent is not required favours employers. Section 7(1)(b) eliminates the consent requirement for the collection of information where obtaining consent would compromise the availability or accuracy of the information, and the collection is for purposes relating to investigating a breach of an agreement or contravention of law. This might allow, for example, an employer to monitor an employee and obtain personal information if the employee is reasonably suspected of theft or other breaches of the employment contract.

6. The PIPED Act in Operation

The Privacy Commissioner has already rendered several decisions regarding allegations by employees of federal works, undertakings or businesses of privacy violations in the workplace. Such decisions have involved, for example, airport authorities, airlines, telecommunications companies, a railway company, a nuclear power corporation.

See Part IV.A.2., An Explanatory Definition of “Personal Information,” above.

2001 Privy Council, the Commissioner’s findings under the PIPED Act, online: <http://www.privcom.gc.ca/fr/cd/cd-de_002109_e.asp>

2002 Privacy Commissioner, the Commissioner’s findings under the PIPED Act, online: <http://www.privcom.gc.ca/cd/cd-de_002107_e.asp>

PPIP Act Case Summary #126: Employer’s Effort to Collect Personal Medical Information Deemed Appropriate; No Evidence of Inappropriate Disclosures (1 February 2003), online: <http://www.privcom.gc.ca/cd/cd-de_002127_1_e.asp>

2003 df cd-de_002127_3 e.asp
potential benefits of, a similar mechanic to employees of federal works.

B. POTENTIAL MODIFICATIONS

Although the cases described above might realize the potential of the PIPA in its existing form, employees might be added to apply specifically to elements discussed above generally in and of individuals and organizations. How considered response to the unique employees is warranted.

For example, it might be prudent ownership of resources ought to have of privacy. It might be beneficial to aspects of privacy in the employee-employer relationship. However, in that particular case, the Commissioner was not convinced that the surveillance measures were justified as necessary, proportionate or effective. Interestingly, in other cases, the Commissioner has disagreed with employers' policies, for example in the context of an employer's disclosure of information to third parties, as well as in respect of an employer's handling of banking information.

Very often, the Commissioner's investigation and recommendations have resulted in quick and effective amendments to the employer's policies and the resolution of the complainant's objections. The apparent efficiency and effectiveness of this process in the federal sphere should serve as additional evidence of the need for, and

145. PIPED Act Cite Summary #65: Emphasize Account of Forcing Consent to Security Screening (14 August 2002), Privacy Commissioner's Findings under the PIPED Act, online: <http://www.privcom.gc.ca/ci-dr/94-de-020814_e.asp>.

146. PIPED Act Cite Summary #66: Employee Opposes Company's Use of Social Insurance Numbers on Forms (9 September 2002), Privacy Commissioner's Findings under the PIPED Act, online: <http://www.privcom.gc.ca/ci-dr/94-de-020904_1_e.asp>.

147. PIPED Act Cite Summary #20, supra note 141.

148. PIPED Act Cite Summary #12, supra note 143.

149. PIPED Act Cite Summary #90, supra note 146.

150. PIPED Act Cite Summary #92, supra note 145.

151. PIPED Act Cite Summary #65, supra note 145.

152. PIPED Act Cite Summary #114, supra note 144.

153. PIPED Act Cite Summary #138, #139, and #120, supra note 143.

154. PIPED Act Cite Summary #65, supra note 145.

155. PIPED Act Cite Summary #118, #139, and #120, supra note 143.

156. PIPED Act Cite Summary #114, supra note 144.

157. PIPED Act Cite Summary #20, supra note 147.

158. PIPED Act Cite Summary #22, supra note 143.

159. See Privacy Protection in the Private Sector: Report of the

160. See Mental Health; Privacy Protection in the
potential benefits of, a similar mechanism that would *not* be limited to employees of federal works.

B. POTENTIAL MODIFICATIONS

Although the cases described above demonstrate that some employees might realize the potential of the PIPED Act if provinces adopted it in its existing form, employees might be even better served if provisions were added to apply specifically in the employment context. The elements discussed above generally balance the competing interests of individuals and organizations. However, a thorough and carefully considered response to the unique concerns of employees and employers is warranted.

For example, it might be prudent to address the effect that ownership of resources ought to have on the reasonable expectation of privacy. It might be beneficial to deal specifically with certain aspects of privacy in the employment relationship, perhaps by identifying situations where it would or would not be appropriate to engage in employee surveillance. Even in situations where this legislation does apply, such as to employees of federal works, undertakings and businesses, it is unclear exactly how employees and employer rights are to be balanced, and which specific invasions might be justifiable. Although existing provisions can fulfill these roles implicitly and indirectly, an express recognition of the issues relevant to employees and employers would more clearly delineate the boundaries of privacy in the employment relationship.

Notably, one of the greatest benefits of adopting provincial legislation is that employees would not need to rely upon the federal Privacy Commissioner located in Ottawa. Indeed, the desire to create a mechanism to deal locally with employee privacy was one of the leading reasons cited by provinces intending to implement provincial legislation. However, it is worth considering whether the Office of the Privacy Commissioner (for each of its provincial counterparts) is best suited to balance the unique competing interests of employees and employers. It might be prudent to utilize the knowledge of those experienced in the labour arbitration field. Such persons could play an invaluable role in the evaluation, mediation, and resolution of complaints, or during the formulation of important policy decisions.

Another concern might be the complexity of the PIPED Act, which has been characterized as awkward, and difficult to interpret and implement. Notably in the federal context, however, much effort has gone into creating user-friendly guides to the legislation, for the benefit of individuals and organizations. Provinces would be

---

119 See Privacy Protection in the Private Sector, supra note 95; Anderton, supra note 94.
160 See Heron, ibid., Privacy Protection in the Private Sector, supra note 95.
wise to follow this example. Nevertheless, additional clarity in the legislation itself is a desirable feature. In sum, although the framework is well-suited to address employee privacy, modifications could more clearly identify the interests at stake and provide stronger and clearer protection for all employees.

V. CONCLUSION

Because employees are vulnerable to invasions of privacy by employers, some form of protection is required. The need for protection is heightened by technological innovation, which allows for easier and more frequent intrusions, and the increasing value of information, which provides incentive for such intrusions to occur.

Lawmakers have accepted this proposition and attempted to establish a legal regime to protect privacy. Although a wide variety of legal mechanisms strive to safeguard the right to privacy in the workplace, none are fully capable of achieving this arduous task. Whereas some forms of protection are only available against privacy intrusions by the government or its agencies, others are only accessible to those with sufficient resources to pursue a remedy. Collective bargaining can alleviate some employees' concerns, but it too assists only a limited number of workers. Generally, the piecemeal privacy protection scheme that currently exists in Canada is inconsistent with the significance attached to this fundamental right.

The PIPED Act illustrates an excellent way in which the privacy rights of non-unionized, private sector employees can be protected. Unfortunately, this PIPED Act does not, and cannot, apply to workers employed by non-federal works, undertakings or businesses. Nevertheless, the positive potential of this legislation can be realized if used as a template upon which provincial legislatures model comparable legislation. Some provinces have taken the initiative to tackle this difficult but important issue. Others should follow those examples. Such laws, if enacted, are the pieces of the puzzle that will complete the picture of privacy protection in Canada.

In Support of Canada's Anti-Terrorism Act: A Comparison of Canadian, British, and American Anti-Terrorism Law

David Jenkins

This article compares Canada's Anti-Terrorism Act to similar British and American legislation, arguing that it is a tempered and positive contribution to the fight against international terrorism. Because terrorism undermines both the values of liberal democracy and international law, an effective legal response requires transnational measures. Accordingly, the shared security concerns and legal culture of Canada, the United Kingdom, and the United States establish a broader context in which to consider their respective anti-terrorism measures and promote informed comparative efforts. The anti-terrorism laws of these three countries similarly define and target terrorist offenses, establish special investigative powers for law enforcement, and attack hate crimes. Examination of their particular statutory provisions suggests that they form complementary legal frameworks for fighting terrorism, to which Canada's Anti-Terrorism Act is a well-drafted and effective contribution.

I. INTRODUCTION

While North Americans may have once thought that they were geographically isolated from political troubles throughout the world and therefore secure from terrorist attacks or activities related to them, the events of September 11 have suddenly and tragically shown otherwise. In a world increasingly connected through communication, transportation, and trade, Canadians and Americans must now confront international terrorism at home. The reality is that extremist groups are willing and able to operate in North America. While the United States is admittedly the most likely target for attack in North America due to its historically strong support of Israel as well as its

* Appro's at Law, B.A., Oshawa, M.A. (Stat.), M.A. (Vol. Sci.), J.D., L.L.M., D.C.L. Candidate, McGill University Institute of Comparative Law. The original version of this article was submitted as a report to the 3rd JUC of Canada. However, the views expressed herein do not necessarily represent those of the organization or any of its staff.