Electronic Employee Monitoring: Potential Reform Options

MELANIE R. BUECKERT*

I. INTRODUCTION

A by-product of the present information economy is the increased use of electronic monitoring technologies in the workplace. As a result, legal reformers are faced with the vexing question of how to best regulate the use of such technologies, particularly in light of the well-known power imbalance that characterizes most employment relationships. This article briefly reviews the existing legislative framework surrounding workplace privacy in Canada and evaluates several potential reform options. In the end, a combination of legal and technological measures may be employees' best protection against the excessive use of electronic employee monitoring technologies by their employers.

A. Defining Electronic Employee Monitoring

The issue of workplace privacy is, like the larger topic of privacy itself, complex and multifaceted. One of the ways in which employees' privacy interests may be engaged in the workplace is through electronic employee monitoring. For the purposes of this paper, the three-prong definition of "electronic monitoring" constructed by Lasprogata, King and Pillay is adopted:

> First, it includes an employer's *use of electronic devices to review and evaluate the performance of employees*. For example, an employer may use a computer to retrieve and review an employee's email messages sent to and from customers in order to evaluate the employee's performance as a customer service representative. Second, it includes *"electronic surveillance"* in the form of an employer's use of electronic devices to observe the actions of employees while employees are not directly performing work tasks, or for a reason other than to measure their work performance. For example, an employer may electronically review an employee's email messages as part of an investigation of a sexual

* Melanie R. Bueckert obtained her LL.B. in 2003, graduating as the gold medalist from the University of Manitoba's Faculty of Law. She was called to the Manitoba bar in 2004 and is currently employed as a legal researcher with the Manitoba Court of Appeal. She earned her LL.M. from the University of Manitoba in 2008, completing her thesis on electronic employee monitoring. Her forthcoming text on the law of employee monitoring in Canada will be published by LexisNexis Canada Inc. in the fall of 2009.

> harassment complaint. ... Third, electronic monitoring includes an employer's use of *computer forensics*, the recovery and reconstruction of electronic data after deletion, concealment, or attempted destruction of the data. For example, an employer may use specialized software to retrieve email messages related to an investigation of alleged theft of its trade secrets by retrieving and reconstructing email messages sent by an employee (the alleged thief) to someone outside the company.[1]

There are a number of reasons why employers rely on electronic employee monitoring technologies.[2] These include:

- productivity (including limiting personal use of company resources (sometimes referred to in relation to the use of computers, internet or e-mail as 'cyber-slacking');
- avoiding legal liability (e.g., for sexual harassment; discrimination; copyright infringement; defamation);
- compliance with workplace policies (such as acceptable computer, internet and e-mail usage);
- prevention or detection of 'moonlighting' or breaches of confidentiality (including corporate espionage);
- prevention of or response to unauthorized access (including hacking into the corporate computer network);
- internet bandwidth regulation and network performance issues;
- network security (which may be threatened by computer viruses and other malware or phishing scams);

---

1 Gail Lasprogata, Nancy J. King & Sukanya Pillay, "Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada" (2004) Stan. Tech. L. Rev. 4 at para. 18 [emphasis added]. Throughout this paper, the terms "monitoring" and "surveillance" are used interchangeably.

2 See e.g. *ibid.* at para. 3; Kris Klein & Vivian Gates, *Privacy in Employment: Control of Personal Information in the Workplace* (Toronto: Thomson Canada Limited, 2005) [Klein and Gates] at 52; Lisa J. Sotto & Elisabeth M. McCarthy, "An Employer's Guide to US Workplace Privacy Issues" (2007) 24 The Computer & Internet Lawyer 1 [Sotto] at 9; Charles Morgan, "Employer Monitoring of Employee Electronic Mail and Internet Use" (1999) 44 McGill L.J. 849 [Morgan] at 852; E. Anne Uteck, *Electronic Surveillance and Workplace Privacy.* (LL.M. Thesis, Dalhousie University Faculty of Law, 2004) [unpublished] at 20-21 [Uteck]; Michael A. Geist, "Computer and E-mail Workplace Surveillance in Canada: The Shift from Reasonable Expectation of Privacy to Reasonable Surveillance" (2003) 82 Can. Bar Rev. 151 at 155; Isabelle Lauzon & Linda Bernier, *La surveillance de vos employés: où, quand, comment?* (Cowansville: Les Éditions Yvon Blais Inc., 2007) at 49-50; Diane Veilleux, "Le droit à la vie privée – sa portée face à la surveillance de l'employeur" (2000) 60 R. du B. 1 at 37; Shelley Wallach, "Who's Info is it Anyway? Employees' Rights to Privacy and Protection of Personal Data in the Workplace" (2007) 23 Int'l J. Comp. Lab. L. & Ind. Rel. 195 at 211; Barbara McIsaac, Rick Shields & Kris Klein, *The Law of Privacy in Canada*, looseleaf (Scarborough: Carswell, 2000) [McIsaac] at 2.5.4.2; Avner Levin, "Big and Little Brother: The Potential Erosion of Workplace Privacy in Canada" (2007) 22 C.J.L.S. 197 [Levin, "Brother"] at 217.

- prevention or detection of unauthorized use of computer systems for criminal or terrorist activities;
- preparation of employer's defence to lawsuits and/or administrative complaints (such as discrimination, harassment or termination);
- response to discovery requests in litigation (electronic evidence);
- vehicle or fleet maintenance;
- employee or public safety; and
- other legal obligations.

However, the mere possibility of employee misconduct is insufficient grounds for electronic monitoring. Many argue that, as in the criminal context, reasonable grounds for suspicion should be shown before any monitoring is undertaken, unless concerns for safety or security are such that they justify indiscriminate monitoring of the workspace.[3]

While there is no doubt that a certain level of supervision is inherent in the employment relationship, "There is a qualitative difference between traditional surveillance and electronic surveillance."[4] This difference often manifests itself in the intensity of the surveillance. While a human supervisor can walk the shop floor and monitor the employees, such surveillance is neither constant nor infallible. Furthermore, the supervisor's memory is not a computer databank, which can be accessed years later to retrieve information that would otherwise never have been captured or remembered about an employee.

This inherent difference between traditional and electronic surveillance is evinced by another common problem related to the electronic monitoring of employees, namely, the subsequent use of information for secondary purposes. The most eloquent explanation of this conundrum is offered by Morin, after citing examples involving a cashier operating a cash register, a truck driver's location being tracked by satellite and a telephone operator's calls being monitored:

---

3 Francis P. Durnford, "Keeping Tabs: The Employer's Right to Monitor Employee Internet and E-mail Activity within the Privacy Law Framework" (2007) 17 E.L.L.R. 65. ("[T]he presence of online distractions such as Facebook are simply not reason enough for employee monitoring...", at 68.) See also Fernand Morin, "Nouvelles technologies et la télésubordination du salarié" (2000) 55 R.I. 725. ("Le risque de quelques maladresses ou l'existence d'un doute relatif à une malversation de la part de certains salariés ne sauraient justifier une surveillance kafkaïenne de tous, partout et à flux continu." at 740)

4 Morgan, *supra* note 2 at 901.

> Ces saisies parallèles des données, ces produits dérivés et les observations pratiques que l'on peut en dégager s'effectuent à l'instar de l'empreinte dans la neige du marcheur: il pose le pied pour avancer et non pas pour y laisser une trace, néanmoins elle s'y trouve...[5]

Ontario's Information and Privacy Commissioner has made use of a similar analogy. Like the popular concept of a "carbon footprint", she refers to the notion of one's "digital footprint", encompassing such things as the websites one visits and one's cell phone usage and credit card activity.[6] It is the path of these digital footprints which employers track using electronic employee monitoring techniques.

B. Technologies Involved in Electronic Employee Monitoring

A number of technologies may be used to electronically monitor employees. The first generation of these tools enabled audio and video surveillance. Employers might monitor their employees' telephone calls, or install video cameras to scan the workplace. As the dynamics of work have changed, computer, internet and e-mail monitoring have come to the fore. The flexibility that new technologies provide to the workforce also means that monitoring employees' locations become important. In mobile workplaces, location awareness technologies like global positioning systems ("GPS") and radio frequency identification ("RFID") are used to track workers' movements. Even in more traditional, non-mobile workplaces, many companies use access cards to monitor their employees' activities. As well, certain workplaces have integrated biometric systems into their access control regimes. Biometrics may also be used to streamline payroll or point-of-sale systems.[7]

Variations and combinations of these technologies are used in a wide variety of workplaces across Canada. It is for this reason that legal reforms regarding electronic employee monitoring are worthy of consideration, particularly given the state of the existing legal regime.

---

5 Morin, *supra* note 3 at 732. See also Levin, "Brother", *supra* note 2 at 218 and Avner Levin *et al.*, *Under the Radar? The Employer Perspective on Workplace Privacy* (June 2006) at 3, online: Ryerson University <http://www.ryerson.ca/tedrogersschool/news/archive/UnderTheRadar.pdf>.

6 Ann Cavoukian, "Technology, Privacy and the Law: The Challenges Ahead" (2006) 7 Internet & E-Commerce Law in Canada 57.

7 Biometric information is derived from an individual's unique measurable biological characteristics, including behavioural and physiological biometrics, and may be used to identify or verify the identity of an individual.

C. Sources of Privacy Law in Canada

Canadian privacy law does not flow from a single source. Instead, it more closely resembles a patchwork quilt, with different laws at the federal and provincial levels and in the public and private spheres.[8] At the highest level, the *Canadian Charter of Rights and Freedoms* (*Charter*) provides a measure of privacy protection to individuals and government employees vis-à-vis the state.[9] Public sector privacy legislation is generally linked to the notion of access to information.[10] The federal government has also enacted certain specific measures to combat the interception of private communications, which may be found in the *Criminal Code*.[11] However, the consent defence attached to these offences essentially renders them impotent in the employment context.

With respect to the private sector, the effectiveness of the federal government's *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)[12] in protecting privacy in the workplace is hampered by Canada's constitutional division of powers between the federal and provincial levels of government.[13] Given that labour and employment are matters under provincial jurisdiction, this federal legislation only extends to employees of federally

---

8 An in-depth review of Canadian privacy law is beyond the scope of this paper. For further background, see McIsaac and Klein, *supra* note 2.

9 Part 1 of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11. Section 32 of the *Charter* delineates the boundaries of its application. Some of the leading cases on privacy under the *Charter* are *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145; *R. v. Dyment*, [1988] 2 S.C.R. 417; *R. v. Duarte*, [1990] 1 S.C.R. 30; *Thomson Newspapers Ltd. v. Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)*, [1990] 1 S.C.R. 425; *R. v. Plant*, [1993] 3 S.C.R. 281; *R. v. Sharpe*, [2001] 1 S.C.R. 45; and *R. v. Tessling*, [2004] 3 S.C.R. 432.

10 *Privacy Act*, R.S.C. 1985, c. P-21; *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165; *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25; *Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01; *The Freedom of Information and Protection of Privacy Act*, S.M. 1997, c. 50; *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31; *An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*, R.S.Q. c. A-2.1; *Protection of Personal Information Act*, S.N.B. 1998, c. P-19.1; *Freedom of Information and Protection of Privacy Act*, S.N.S. 1993, c. 5; *Freedom of Information and Protection of Privacy Act*, R.S.P.E.I. 1988, c. F-15.01; *Access to Information and Protection of Privacy Act*, S.N.L. 2002, c. A-1.1; *Access to Information and Protection of Privacy Act*, R.S.Y. 2002, c. 1; *Access to Information and Protection of Privacy Act*, S.N.W.T. 1994, c. 20.

11 R.S.C. 1985, c. C-46, ss. 184, 342.1(1)(b).

12 S.C. 2000, c. 5.

13 *Constitution Act, 1867* (U.K.), 30 & 31 Vict., c. 3, reprinted in R.S.C. 1985, App. II, No. 5, ss. 91, 92.

regulated works, undertakings and businesses.[14] Complementary provincial legislation is therefore required to furnish other employees with a similar level of privacy protection.[15]

Before these types of comprehensive data protection regimes were implemented, statutory invasion of privacy torts were introduced in several provinces.[16] However, due to the often prohibitive cost of litigation, reliance has not often been placed upon these statutes. Also, as with the *Criminal Code* provisions mentioned above, the broad consent defence contained in these statutes renders them effectively inapplicable to the workplace context.[17] Similarly, there has been limited development of the common law of privacy in Canada.[18]

D. Summary of the Manitoba Position

In Manitoba, as elsewhere in Canada, *Charter* privacy protections are available to government employees. Public sector freedom of information and protection of privacy legislation has also been in place for some time.[19] A similar regime applies to trustees of personal health information.[20] *PIPEDA* applies to employees of federal works, undertakings and businesses. While substantially similar private

---

14 *Supra* note 10, s. 4(1)(b). The phrase "federal work, undertaking or business" is defined in s. 2(1).

15 Three provinces have enacted private sector privacy legislation that is substantially similar to *PIPEDA* (*supra*, note 10), namely, British Columbia (*Personal Information Protection Act*, S.B.C. 2003, c. 63 [BC *PIPA*]), Alberta (*Personal Information Protection Act*, S.A. 2003, c. P-6.5 [AB *PIPA*]) and Quebec (*An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-39.1). Ontario's health privacy legislation, *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, Sch. A, has also been recognized as substantially similar to *PIPEDA*, but it is not relevant for the purposes of this paper.

16 Such legislation exists in four of Canada's common law provinces, namely, British Columbia (*Privacy Act*, R.S.B.C. 1996, c. 373), Manitoba (*The Privacy Act*, R.S.M. 1987, c. P125 *The Privacy Act*), Newfoundland and Labrador (*Privacy Act*, R.S.N. 1990, c. P-22) and Saskatchewan (*Privacy Act*, R.S.S. 1978, c. P-24). These initiatives were inspired by the work of the Uniform Law Conference of Canada <http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1p3>.

17 See e.g. *The Privacy Act*, *ibid.*, s. 5(a).

18 See e.g. Geoffrey England, *Individual Employment Law* (Toronto: Irwin Law, 2000) at 139 and Geoffrey England & Roderick Wood, *Employment Law in Canada*, 4th ed., looseleaf (Markham: LexisNexis Butterworths, 2005) at §8.271.

19 *The Freedom of Information and Protection of Privacy Act*, *supra* note 10.

20 *The Personal Health Information Act*, S.M. 1997, c. 51.

sector privacy legislation has been proposed, it has not yet been implemented.[21] Some limited protection of employees' personal information is provided by *The Personal Investigations Act*.[22] However, that Act defines a "personal investigation", in part, as "any inquiry by any person to obtain factual or investigative information from any source other than the subject with a view to entering into or amending an agreement with the subject for credit, insurance, employment or tenancy... ."[23] For this reason, it does not appear that electronic employee monitoring conducted during the course of the employment relationship, without a view to amending the existing employment agreement, would be affected by this legislation.

E. Options for Reform

Thus, as can be seen, there is a large gap in the legal protections currently available to employees subjected to electronic monitoring by their employers in Canada. Reform is required to remedy this gap in employees' privacy protections. There are numerous options that could be explored, namely: (1) employee privacy education campaigns and greater industry self-regulation; (2) enactment of substantially similar private sector privacy laws in all provinces, modeled after those in British Columbia, Alberta and Quebec; (3) amendment of existing employment standards legislation to address the issue of electronic employee monitoring; (4) enactment of stand-alone surveillance legislation, governing employees as well as all other members of society; and (5) amendment of the *Criminal Code* to specifically address the issue of electronic employee monitoring. Each of these options will be examined in turn.

1. Improved Employee Education and Greater Industry Self-Regulation

The least drastic reform option would involve a public education campaign, explaining to employees that they have the ability to bargain for increased privacy protections in the workplace. The primary drawback associated with this less aggressive approach is that it does little to alter the power imbalance characteristic of most employment relationships. Those employees who are already able to negotiate privacy protections on their own behalf will not likely be greatly assisted by such a campaign; moreover, it would not likely alter the position of employees who currently lack the bargaining power to seek privacy protections from their employers.

---

21 Bill 216, *The Personal Information Protection and Identity Theft Prevention Act*, 2nd Sess., 39th Leg., 2007. In the interests of full disclosure, it should be noted that the author was involved with the drafting of Bill 216

22 R.S.M. 1987, c. P34.

23 *Ibid.*, s. 1.

Greater industry self-regulation is unlikely, except as a last-ditch attempt to avoid the imposition of more stringent legislative provisions or as a prophylactic measure against increased unionization driven by employee privacy concerns. As neither of these scenarios currently exists in Canada, it does not appear that greater industry self-regulation will occur in the near future.

2. The Role of Unions

Given the current state of the law regarding electronic employee monitoring in Canada, unions have the opportunity to play an important role in upholding employees' privacy interests in the workplace.[24] Whether or not they will do so, or will succeed in doing so, is still an open question. Unfortunately, there does not appear to be a great deal of legal scholarship on this particular aspect of workplace privacy in Canada. One of the most thorough studies of the issue was undertaken by Kiss and Mosco in 2004. They searched the Human Resources and Skills Development Canada database, which contains 5 495 representative collective agreements from across Canada, in order to determine the extent to which such agreements included express provisions regarding electronic surveillance—their research revealed 76 agreements.[25]

Their work followed-up on a similar study conducted in 1995 which showed virtually no response by unions to electronic surveillance practices in the workplace. As such, they concluded that "some progress is being made"[26] but "developments in this area are slow."[27] Kiss and Mosco adopted the following hypothesis regarding the limited number of collective agreements containing provisions that dealt with electronic surveillance uncovered by their research:

> A number of reasons could explain the limited response by Canadian unions [to electronic surveillance practices in the workplace]. The relative decline of the industrial economy in which unions thrived has challenged the very survival of numerous unions in North America. The growth of a large temporary workforce and of companies such as Wal-Mart that are skilled in the use of new technologies to cut costs has posed serious problems for traditional unions. Like their American counterparts Canadian unions have had to focus on fundamental issues like job security, wages, and organizing. Important as privacy is, and most unions recognize the problem that surveillance poses, unions have chosen to place it lower on the list of policy priorities. Furthermore, although this is changing, electronic surveillance and privacy have historically been applied to women workers such as telephone operators and data entry workers, whose limited power in

---

24 Simon Kiss & Vincent Mosco, "Negotiating Electronic Surveillance in the Workplace: A Study of Collective Agreements in Canada" (2005) 30 Canadian Journal of Communication 549. ("[C]ollective bargaining offers unions a wide range of options to structure, limit, influence, and control..." the practice of electronic employee monitoring, at 562).

25 *Ibid.* at 550. This translates to approximately 1.4%.

26 *Ibid.* at 555.

27 *Ibid.* at 553.

> unions has made it all the more difficult to give surveillance a more prominent place on the trade unions[']agenda.[28]

Further:

> Limited attention to surveillance may be a function of surveillance's lower status in the hierarchy of trade union and worker bargaining priorities. It is not implausible to imagine trade unions conceding surveillance measures in return for job and wage protection. Alternatively, it may be that the pace of technological change is outstripping union ability to integrate these changes into bargaining processes.[29]

Kiss and Mosco found that public sector unions had been more successful in obtaining collective agreement protection from electronic monitoring than their private sector counterparts. As they observed, "[t]his is not a surprising finding. First, the Canadian public sector boasts a higher unionization rate than the private sector. Second, postsecondary education unions have particular concerns about privacy and anti-surveillance measures that contribute to the observed predominance of public-sector unions."[30]

The two most represented national unions in the sample were the Canadian Auto Workers (C.A.W.) and the Canadian Union of Public Employees (C.U.P.E). University faculty unions made up the third largest group of unions with surveillance-related collective agreement provisions. Again, this finding is not surprising, as C.A.W. and C.U.P.E. are two of the three largest unions in Canada.[31] In addition, Kiss and Mosco found that "some of the strongest language stems from agreements between unions as employers and unions that represent the union's employees."[32]

Kiss and Mosco discerned four types of surveillance-related clauses, which they described as "low privacy protection",[33] "moderate privacy protection",[34] "high privacy protection"[35] and "worker-friendly surveillance."[36] The low category "included cases where the employer was explicitly empowered to engage in surveillance activities or where the only restriction on surveillance was a

---

28 *Ibid.* at 555-556.

29 *Ibid.* at 561.

30 *Ibid.* at 556, which includes a table that sets out their findings by language and public versus private sector.

31 *Ibid.*, which includes a table that sets out their findings by industrial sector.

32 *Ibid.* at 560.

33 *Ibid.* at 558.

34 *Ibid.* at 558.

35 *Ibid.* at 558.

36 *Ibid.* at 558.

matter of informing employees."[37] The moderate level included clauses that accepted existing surveillance practices but sought to impose some limits, "such as a halt to further expansion of surveillance activities."[38] Generally speaking, moderate provisions accepted electronic monitoring in general, but sought to prevent its use for keeping track of individual workers' pace or productivity. The high category included clauses that severely limited surveillance practices, most often only to the prosecution of criminal offences. These clauses were usually structured as a guarantee that surveillance would not be used, except in narrowly defined situations. The worker-friendly category captured collective agreement language, which permitted surveillance for the purposes of worker safety and protection of their property.[39]

Whether a particular provision engenders worker-friendly surveillance would seem to be open for debate. Indeed, with slightly different drafting or "spin", such a provision could well constitute a low level of worker property protection. In addition, initially permitting surveillance under the guise of worker safety or protection may make it easier for surveillance to be used for other purposes in the future (*i.e.*, may facilitate 'function creep'). From the perspective of protecting workers' privacy, it is not at all clear that these types of "worker friendly" provisions are indeed in the long-term interests of employees, or whether they are even objectively comparable with other forms of collective agreement provisions on the topic of electronic surveillance.

After their extensive review of these collective agreements, Kiss and Mosco summarized the approaches that may be taken to electronic monitoring in collective agreements, in the following manner:

- Unions can allow surveillance practices and defer to management.
- Unions can insist on signage in the workplace, informing employees and customers of the presence of surveillance technologies.
- Unions can require that the employer inform the union about the introduction of surveillance practices.

---

37 *Ibid.* at 558.

38 *Ibid.* at 558.

39 *Ibid.* at 558-559, which includes a table showing the breakdown of the collective agreements by category. Of the 76 agreements classified, 32 fell within the moderate category while 24 were captured by the high category, together combining for nearly three-quarters of all of the agreements reviewed. There were five worker-friendly agreements, which represented less than 10% of the total sample. As Kiss and Mosco note at 561, "Although surveillance practices can be put in place to protect the interests of employees, the overwhelming majority of collective agreement clauses on the matter involved unions attempting to restrict employers' use of electronic surveillance practices."

- Surveillance practices can be prohibited or prohibited save for criminal investigations.
- Unions can insist that surveillance technologies be put in place to protect workers' health, safety, and property.
- Unions can prevent data gathered by electronic means from being used in productivity evaluation or criminal proceedings.
- Unions can require that information above and beyond what was gathered by electronic means be used in any disciplinary or criminal proceeding.
- Unions can require that employees be informed when they will be monitored electronically or unions can require the consent of individuals before surveillance can take place.[40]

Kiss and Mosco reached the eminently reasonable and arguably self-evident conclusion that "there is reason to expect growth in the number of collective agreements covering electronic surveillance" in the coming years.[41] It would seem equally reasonable to assert, based on their research, that such agreements will continue the trend of predominantly favouring moderate or high levels of employee privacy protection, perhaps in even greater percentages. If other methods of workplace privacy law reform do not move forward, more employees may turn to unions to protect themselves.

3. Enactment of Substantially Similar Private Sector Privacy Legislation in All Provinces

Another potential avenue for reform would be the enactment of substantially similar private sector privacy legislation in all of the provinces. While it would involve the passage of new legislation, this option for reform would require the least amount of political effort, as the necessary templates have already been developed in British Columbia, Alberta and Quebec.[42] For instance, Manitoba's Bill 216 borrows heavily from Alberta's private sector privacy legislation.[43]

While private sector legislation addressing electronic employee monitoring need not be substantially similar to *PIPEDA* in other respects, if it were broadened enough to cross the "substantially similar" threshold, this type of reform would have the added benefit of simplifying the privacy law regime to

---

40 *Ibid.* at 561.

41 *Ibid.* at 562.

42 *Supra* note 15.

43 *Supra* note 21.

which private sector organizations are subject.[44] Instead of having a federal law regulating consumer privacy and a provincial law regulating employee privacy, a substantially similar provincial private sector privacy law could regulate both consumer and employee privacy.

This approach to reform has the additional benefit of addressing all aspects of employee privacy, rather than only targeting electronic monitoring. It would also avoid the pitfall of being technology-specific and would likely be drafted broadly enough so as to be capable of anticipating and expanding to meet future challenges.[45] If legislation is tied to specific forms of technology, then it must be constantly updated to address new technological developments. In this way, the law is relegated to a reactive role, always trying to keep pace with advances in technology. While no legislation can accurately predict and regulate future developments, more broadly drafted proactive legislation can provide guidance and some degree of certainty when new technologies are introduced. While technological developments may require legislative amendment, at least the framework for addressing the new technology would already be clearly established.

The primary difficulty associated with the enactment of private sector privacy legislation relates to enforcement. To date, it would appear that an ombudsperson-type role has been accepted as appropriate in the context of the access to information regime. This model has been extended into the data protection realm. While accessibility is a mandatory component of any effective privacy protection regime, it is questionable whether the existing ombudsperson-

---

[44] According to s. 26(2)(b) of *PIPEDA*, if a province enacts substantially similar legislation, *PIPEDA* ceases to apply in that province.

[45] A prime example of piecemeal technology-specific legislation is the RFID measures implemented in several American states. Several American states have passed legislation banning the forced implantation of RFID chips into employees, in response to certain employers making such implantation a mandatory condition of employment. Wisconsin, North Dakota and California have all passed laws prohibiting forced RFID implantation. See, Anita Ramasastry, "Outlawing Employer Requirements that Workers Get RFID Chip Implants: Why It's the Right Thing for States to Do, Although Current Statutes May Need Refinement" (16 October 2007), online: Writ <http://writ.news.findlaw.com/ramasastry/ 20071016.html>. Voluntary implantation is still permissible. The state of Washington has since passed a broader bill aimed at RFID technology more generally. See, *Electronic Communication Devices*, c. 138, 2008 Wash. Acts <http://apps.leg.wa.gov/documents/billdocs/2007-08/Pdf/Bills/Session%20Law%202008/1031-S.SL.pdf>. At the time of writing, Alaska and New Hampshire were considering similar legislation. See, "Washington Passes First Radio Frequency ID Law" *Adlaw* (15 May 2008), online: Reed Smith <http://www.adlawbyrequest.com/legislation.cfm?cit_id=2938&FaArea2=customWidgets.content_view_1&usecache=false&ocl_id= ARTICLE>. See also "2008 Privacy Legislation Related to Radio Frequency Identification" (3 July 2008), online: National Conference of State Legislatures <http://www.ncsl.org/programs/lis/privacy/rfid08.htm>.

based model is best suited to this area of the law. At the very least, privacy commissioners should be granted the power to make orders that are enforceable like court orders.[46] So long as legislators are unwilling to provide privacy commissioners and their staff with these types of enforcement powers, other intermediate reform measures must be considered.

4. Amendment of Existing Employment Standards Regimes

In answer to the enforcement concerns raised by the reform option of enacting substantially similar private sector privacy legislation, the main benefit of achieving reform through amendments to existing employment standards legislation is that enforcement mechanisms are already well-established under such regimes. While additional resources would be required to properly operate and maintain such an expanded system, the basic structure for making complaints and appealing decisions is already in place. Like the possibility of enacting private sector privacy legislation, this reform option would preserve accessibility, as it relies upon an informal administrative process rather than expensive litigation.

The main problem with this reform option is that employment standards officers are not workplace privacy experts. While they could develop this expertise over time, it is debatable whether privacy, which some view as a fundamental human right, is properly adjudicated in this type of practical, pragmatic forum. In order to counteract this criticism, any legal reforms along these lines would have to ensure that sufficiently broad remedial powers were granted to employment standards personnel, to make systemic remedies similar to those associated with human rights regimes available to solve these types of workplace privacy problems.

5. Enactment of Stand-alone Surveillance Legislation

Another possibility for reform is the enactment of stand-alone surveillance legislation. Like private sector privacy legislation, this type of surveillance statute would not necessarily be confined to the employment context. Specifically, a provincial government could pass legislation that defines surveillance, indicates that surveillance without consent is prohibited except in certain circumstances, and sets out those exceptions. It might even distinguish between covert and

---

[46] This power has been given to the Information and Privacy Commissioners of British Columbia and Alberta, but not the federal Privacy Commissioner. See, BC *PIPA* (*supra* note 14) Part 11; AB *PIPA* (*supra* note 14), Part 5 (particularly s. 52(6)); *PIPEDA* (*supra* note 10), Part 1, Division 2.

overt surveillance. This is the reform approach that has been advocated in Australia.[47]

If such legislation were to be implemented in Canada, useful guidance could be obtained from the existing Australian legislation on this subject.[48] For instance, New South Wales' *Workplace Surveillance Act 2005* defines "surveillance" as follows:

> "[S]urveillance" of an employee means surveillance of an employee by any of the following means:
> (a) "camera surveillance", which is surveillance by means of a camera that monitors or records visual images of activities on premises or in any other place,
> (b) "computer surveillance", which is surveillance by means of software or other equipment that monitors or records the information input or output, or other use, of a computer (including, but not limited to, the sending and receipt of emails and the accessing of Internet websites),
> (c) "tracking surveillance", which is surveillance by means of an electronic device the primary purpose of which is to monitor or record geographical location or movement (such as a Global Positioning System tracking device).[49]

The same section defines "surveillance information" to mean "information obtained, recorded, monitored or observed as a consequence of surveillance of an employee". Subsection 5(1) confirms that the phrase "at work" is meant to be construed liberally:

> For the purposes of this Act, an employee is "at work" for an employer when the employee is:
> (a) at a workplace of the employer (or a related corporation of the employer) whether or not the employee is actually performing work at the time, or
> (b) at any other place while performing work for the employer (or a related corporation of the employer).

The legislation goes on to address the notification of employees regarding workplace surveillance,[50] prohibited surveillance,[51] as well as covert surveillance.[52]

One potential pitfall with this type of legislative reform is that, of the reform options identified herein, it is the most susceptible to losing its technological

---

47 See e.g. New South Wales Law Reform Commission, *Surveillance: An Interim Report* (Sydney: New South Wales Law Reform Commission, 2001) and Victorian Law Reform Commission, *Workplace Privacy: Final Report* (Melbourne: Victorian Law Reform Commission, 2005).

48 See e.g. *Surveillance Devices Act 1999* (Vic.), as am. by *Surveillance Devices (Workplace Privacy) Act 2006* (Vic.); *Workplace Surveillance Act 2005* (N.S.W.); *Surveillance Devices Act 2007* (N.S.W.).

49 *Ibid.*, s. 3.

50 Part 2, ss. 9-14.

51 Part 3, ss. 15-18.

52 Part 4, ss. 19-38.

neutrality. In drafting any such regime, care would have to be taken to keep the definition of surveillance as broad as possible, without being tied to existing technologies.

Furthermore, it is uncertain whether this form of legislative initiative would adequately address the privacy implications of biometrics. If this path to legislative reform is followed, companion legislation regarding the use of biometrics in the workplace (or more generally) may also have to be implemented.[53]

6. Additional Criminal Code Provisions

One final potential avenue for reform is the enactment of specific *Criminal Code* provisions to address electronic employee monitoring. However, given the lacklustre track record of the existing *Criminal Code* provisions regarding the interception of electronic communications, it seems unlike that this would be a fruitful law reform exercise.[54] While new provisions could be added without broad consent defences, specifically for the purpose of protecting employees' privacy, the fact that enforcement would remain a public matter would likely deprive affected employees of any significant personal remedy. However, the threat of a criminal prosecution might be the necessary incentive for employers to take employee privacy issues seriously.

A further potential difficulty with this type of reform is that any such amendments might be seen as colourable attempts on the part of the federal government to regulate employment matters, which are properly within the jurisdiction of the provinces. As such, this type of legislative provision could be open to a constitutional challenge.[55]

---

[53] A useful starting point for such legislation may be found in ss. 44 and 45 of Quebec's *Act to establish a legal framework for information technology*, R.S.Q. c. C-1.1. However, the availability of a consent defence should be re-examined in the workplace context.

[54] The American experience with similar legislation, the *Electronic Communications Privacy Act of 1986*, P.L. 99-508, confirms that this is not a viable path to reform. See e.g. Klein and Gates, *supra* note 2 at 53-55; Karen Eltis, "The Emerging American Approach to E-mail Privacy in the Workplace: Its Influence on Developing Caselaw in Canada and Israel: Should Others Follow Suit?" (2003) 24 Comp. Lab. L. & Pol'y J. 487; Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law* (Charlottesville: Michie, 1996) at 374-375; Lasprogata, *supra* note 1; Sotto, *supra* note 2.

[55] In fact, Quebec has already challenged the constitutional validity of *PIPEDA*, *supra* note 10. See Quebec Order-in-Council No. 1368-2003-12-30 (English version available online at http://www.steptoe.com/assets/ attachments/603.pdf) dated December 17, 2003; the Quebec Court of Appeal file number is 500-09-014067-037. A decision has not yet been rendered in the matter.

II. CONCLUSION

Given the limited protection presently granted to employees' privacy interests, it would seem that any effective reforms will require major legislative intervention, not just incremental judicial change. Three viable avenues are (1) the enactment of private sector privacy laws in all of the provinces (which may or may not be substantially similar to *PIPEDA*[56]), which specifically address the topic of electronic employee monitoring; (2) the inclusion of privacy protections in existing employment standards legislation across Canada;[57] or (3) the enactment of stand-alone surveillance legislation.

Each of these three potential initiatives emanates from a different core. Private sector privacy legislation places the emphasis on privacy; amendments to existing employment standards regimes would merely be an outgrowth of employment law; and the enactment of stand-alone surveillance legislation would be primarily focused on the protection of individuals from the evils of surveillance. Given that any such legislative reforms would have to be politically motivated, the trend of public opinion and the impetus for the reform would likely dictate which of these three models was chosen.

Regardless of which route is taken, the accessibility of the regime must be ensured and effective remedial powers given to its enforcers. The implementation of additional unjust dismissal regimes or the creation of specialized labour courts could assist in achieving both of these objectives. As Uteck observes:

> What is at stake in the privacy debate is not so much the claim to protect the individual employee from privacy invasions, as the establishment of ground rules and limits of acceptable institutional behaviour in the context of rapid changes in the technologies of surveillance and information technology.[58]

Guidance in this task may be taken from international developments, including the legislative approaches to electronic employee monitoring adopted by other countries. For instance, Canadians should learn from the United States' experience with the ECPA and its tendency to implement technology-specific, reactive legislation. Conversely, the in-depth surveillance studies undertaken by

---

56 *Supra*, note 12.

57 As England observes in *Individual Employment Law*, *supra* note 18 at 139: "Canadian employment standards acts currently do not contain comprehensive safeguards against undue interference by employers with the privacy of their employees. This situation may change if employers are perceived to be abusing the various technologies that potentially create such a risk, such as video monitoring, computerized files, and electronic and voice mail."

58 Uteck, *supra* note 2 at 183. This is another reason why piecemeal technology-specific reforms should be avoided.

law reform commissions in Australia, and the resulting legislative initiatives, should receive careful consideration if similar legislation is advocated in Canada.

If legal reformers fail to pursue these options, employees will be required to either accept violations of their privacy in the workplace or rely on technological measures to combat such incursions. This would mean that more tech-savvy employees, or at least those with access to greater resources, would benefit from better workplace privacy protections. This inequitable result could be avoided through law reform, which would serve to level the workplace privacy playing field.

Nevertheless, lawyers ought to consider the role to be played by such privacy protection technologies when drafting legislation dealing with electronic employee monitoring. For instance, a workplace surveillance law could state that an employee's use of privacy protection technologies (such as anonymous proxy servers or encryption programs) does not, by itself, constitute grounds for enhanced surveillance or scrutiny of their activities. Such legislation might also include a non-retaliation clause, similar to whistleblower protections contained in other legislation, for employees who chose to arm themselves with technological protections against privacy invasions in the workplace.

Generally speaking, law reform initiatives should attempt to see beyond the latest technological developments to assist in crafting laws that anticipate future technological advancements, rather than relegating law reform to a reactive 'catch-up' exercise. At the same time, in some cases, law reform objectives may be more quickly and easily obtained through reliance on appropriate technologies. With respect to electronic employee monitoring, an appropriate fusion of legal reform and privacy protection technologies may be the ultimate solution to this complex legal problem.