Watching Workers

A Critical Review of the Law Regarding Electronic Employee Monitoring in Non-Unionized Workplaces in Canada

Prepared by
Melanie R. Bueckert

A Thesis submitted to the Faculty of Graduate Studies of
the University of Manitoba
in partial fulfillment of the requirements of the degree of

MASTER OF LAWS

Faculty of Law
University of Manitoba
Winnipeg

ABSTRACT

This thesis addresses the topic of electronic employee monitoring in non-unionized workplaces in Canada. Electronic employee monitoring is defined as including (1) the use of electronic devices to review and evaluate employees' performance; (2) 'electronic surveillance'; and (3) employers' use of computer forensics. Detailed consideration is given to a variety of technologies, including computer, internet and e-mail monitoring, location awareness technologies (such as global positioning systems and radio frequency identification), as well as biometrics, and the developing case law surrounding these innovations. Analogies are drawn to the jurisprudence developing with respect to unionized workplaces and under statutory unjust dismissal regimes.

This analysis leads to the conclusion that legislative reform is necessary, either through (1) the creation of parallel private sector privacy regimes, such as those in British Columbia and Alberta, mirroring existing federal legislation; (2) amendments to existing employment standards legislation; or (3) the enactment of a stand-alone surveillance statute.

ACKNOWLEDGEMENTS

I would like to take this opportunity to thank my advisor, Dr. Bryan Schwartz, for his guidance and direction in the completion of this program of study and, more generally, for his role in shaping my career path. I also wish to thank Prof. Debra Parkes for her thoughtful comments as my internal reviewer. I am indebted to Dr. Michael Geist of the University of Ottawa's Faculty of Law for acting as my external reviewer.

I received exceptional support from Dr. Michelle Gallant, Associate Dean of Research and Graduate Studies for the University of Manitoba's Faculty of Law, which epitomized the encouragement I received from other members of the Faculty and the assistance I was given by the Faculty's support staff. In particular, I wish to express my thanks to Prof. Anne McGillivray for broadening my horizons through the Graduate Legal Research and Theory course. My special thanks also extend to John Eaton, Gail Mackisey, Wendy Prystenski, Regena Rumancik, Muriel St. John and Sean Watson of the E. K. Williams Law Library for their assistance with my many questions and queries.

My pursuit of this degree was greatly aided by the financial support I received from the Faculty of Law in the form of the Freedman and Sgayias Fellowships. I am also grateful for the flexibility shown by my employer, the Manitoba Court of Appeal, in accommodating my academic pursuits.

Last but certainly not least I thank my family and friends for bearing with me while I was completing my degree requirements and for listening to my endless ramblings about workplace privacy. Thank you for your patience!

DEDICATION

To Sean, my wonderful husband and friend, for being there every step of the way

To my parents, for their unwavering love, support and encouragement

God, in all I do, I try to honour You (Psalm 40:8; Colossians 3:17)

TABLE OF CONTENTS

I. Introduction

> Work is one of the most fundamental aspects in a person's life, providing the individual with a means of financial support and, as importantly, a contributory role in society. A person's employment is an essential component of his or her sense of identity, self-worth and emotional well-being. Accordingly, **the conditions in which a person works are highly significant in shaping the whole compendium of psychological, emotional and physical elements of a person's dignity and self respect**.[1]

One such 'employment condition' is employees' privacy. Generally speaking, "[t]he judicial and legislative trend in Canada is toward ever greater protection of individual privacy rights...".[2] As deBeer explains, "[s]ociety 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."[3]

The issue of employee privacy is by no means new; as Flaherty notes, "…industrialization has brought wave after wave of challenges to personal privacy, each of which [p. 190] required some kind of balancing of competing rights."[4] However, with the growth of the information economy and the resultant blending of personal and private time and space, the employee privacy issues raised by electronic monitoring have come to the fore. Two competing societal

---

[1] *Reference Re Public Service Employee Relations Act (Alta.)*, [1987] 1 S.C.R. 313 at 368, Dickson C.J.C. [emphasis added].

[2] Charles Morgan, "Employer Monitoring of Employee Electronic Mail and Internet Use" (1999) 44 McGill L.J. 849 [Morgan] at 854.

[3] Jeremy deBeer, "Employee Privacy: The Need for Comprehensive Protection" (2003) 66 Sask. L. Rev. 383 [deBeer] at 383. Indeed, it is often remarked that the workplace is a microcosm of society at-large: see e.g. Eugene Oscapella, "Workplace Surveillance: Serving the Omniscient State" (1998) 6 C.L.E.L.J. 341 [Oscapella] at 341.

[4] David H. Flaherty, "Workplace Surveillance: The Emerging Reality" (1992) Lab. Arb. Y.B. 189 at 189-190. As Uteck observes, "High tech, low privacy may be an apt description of the 21st century workplace": E. Anne Uteck, *Electronic Surveillance and Workplace Privacy.* (LL.M. Thesis, Dalhousie University Faculty of Law, 2004) [unpublished] at 4 [Uteck].

trends underlie this state of affairs: as computing in the workplace becomes more entrenched, surveillance seems to develop apace; however, privacy is emerging as a cherished societal value, which individuals do not wish to surrender without ample justification.[5]

This thesis examines the current state of the law in Canada regarding electronic employee monitoring in non-unionized workplaces. It also explores potential avenues for legal reform, with a view to strengthening the legal protections provided to employees' privacy interests.

II. Defining Workplace Privacy

The legal dimension of electronic employee monitoring primarily relates to workplace privacy interests, and the extent to which employee privacy concerns should yield to other competing demands. In order to place this legal issue in context, it is useful to undertake an analysis of the underlying concept of workplace privacy. This, in turn, requires a basic understanding of the broader notion of "privacy" generally.

Unfortunately, despite a variety of attempts, "a workable definition of privacy remains elusive."[6] As Lawson and Jeffery observe, "[p]rivacy has been addressed as a 'right,' a 'value,' an 'interest,' a 'claim,' a 'condition,' a 'principle,' an 'ability,' a 'power,' and of course, 'a constellation of values, claims and

[5] 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 [Geist] at 177-178.
[6] Uteck, *supra* note 4 at 54.

interests in a universe of concurring and competing values.'"[7] The concept of privacy is multifaceted:

> …it is a bundle of not very clearly defined rights and expectations according to which individuals should have some degree of intimacy, secrecy, dignity, autonomy, or independence; and perhaps should enjoy a right to be left alone, to control what others know about them, or simply to be themselves.[8]

Generally speaking, approaches to the meaning of privacy may be categorized into four groups: anti-interventionism; informational self-determination; legal pragmatism; and definitional agnosticism. Anti-interventionists conceptualize privacy as a right to be free from interference. Westin, a well-known proponent of the informational self-determinism approach to privacy, defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[9] Representative of legal pragmatists, Schafer offers the following definition of privacy, which is adopted for the purpose of this thesis:

> Any very precise definition would misrepresent the fuzzy edges which the concept has in actual usage. My proposal is that the term 'privacy' can be defined by combining our two conditions: (1) control over information about oneself and over who can sense us, and (2) non-interference in private affairs.[10]

---

[7] Ian Lawson & Bill Jeffery, *Privacy and Free Enterprise: The Legal Protection of Personal Information in the Private Sector*, 2nd ed. (Ottawa: Public Interest Advocacy Centre, 1997) [Lawson] at 57. At 76, Uteck, *ibid.* states: "Different categories have been advanced as possible means for explaining or protecting privacy: privacy as a right, as a claim, as an interest, as an aspect of control and as a state or condition." The characterization of privacy as a "right" in the employment context is discussed in greater detail, below.

[8] Mark Jeffery, "Information Technology and Workers' Privacy: Introduction" (2002) 23 Comp. Lab. L. & Pol'y J. 251 at 262.

[9] Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967) at 7.

[10] Arthur Schafer, "Privacy: A Philosophical Overview" in Dale Gibson, ed., *Aspects of Privacy Law: Essays in Honour of John M. Sharp* (Scarborough: Butterworth & Co. (Canada) Ltd., 1980) 1 at 14. This is similar to the simple definition offered by George Radwanski, "Workplace Privacy: A New Act, a New Era" (2001-2002) 2 Lab. Arb. Y.B. 1 [Radwanski] at 6. The most famous proponents of the "non-interference" approach to privacy are Samuel Warren and Louis Brandeis. See "The Right to Privacy" (1890) 4 Harv. L. Rev. 193, where they define privacy as "the right to

Lastly, in the face of voluminous conflicting academic opinions on the subject, definitional agnostics "reject entirely the effort to arrive at an absolute definition" of privacy.[11] Definitional agnosticism posits that "[p]rivacy is a derivative interest that flows from other legally cognizable, conceptually dissimilar rights or claims, or a state of being – not a right *per se*."[12] Definitional agnostics often refer to privacy as a 'cluster concept', meaning that it is a group of otherwise self-sustaining rights and does not have any unique independent meaning.

The only aspect of privacy about which there is a consensus is the fact that, whatever it is, it is not absolute.[13] It is also generally conceded that privacy is highly context-driven, and it is for this reason that workplace privacy must be considered separately, as a distinct subset of the broader concept of privacy in general.[14]

In *R. v. Dyment*, Mr. Justice La Forest referred to three "spheres" of privacy, namely, spatial/territorial, personal and informational.[15] In the workplace privacy context, particularly with regard to electronic monitoring, the aspect of privacy most often at issue is the informational sphere. For instance, McIsaac,

---

be let alone". Mr. Justice Brandeis' dissenting judgment in *Olmstead v. U.S.*, 277 U.S. 438 (1928) is another oft-quoted source for this view.

[11] Lawson, *supra* note 7 at 45.

[12] *Ibid.* at 54.

[13] See e.g. 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 [Wallach] at 203; Morgan, *supra* note 2 at 859-860 and 888; Isabelle Lauzon & Linda Bernier, *La surveillance de vos employés: où, quand, comment?* (Cowansville: Les Éditions Yvon Blais Inc., 2007) [Lauzon] at 1; Diane Veilleux, "Le droit à la vie privée – sa portée face à la surveillance de l'employeur" (2000) 60 R. du B. 1 [Veilleux] at 45.

[14] See e.g. Morgan, *ibid.* at 859 and Avner Levin *et al.*, *Under the Radar? The Employer Perspective on Workplace Privacy* (June 2006), online: Ryerson University <http://www.ryerson.ca/tedrogersschool/news/archive/UnderTheRadar.pdf> [*Under the Radar*] at 3.

[15] [1988] 2 S.C.R. 417, especially paras. 19 and 34. This taxonomy was endorsed more recently by Mr. Justice Binnie in *R. v. Tessling*, [2004] 3 S.C.R. 432 at para. 20, though in para. 25 he also noted that "Privacy is a protean concept...".

Shields and Klein state that "[t]he phrase 'workplace privacy' encompasses an employer's collection, use and disclosure of information about their employees."[16] Ford explains that the employer's privacy issues also tend to relate to informational privacy, and are protected by the law relating to trade secrets, breach of confidence and fiduciary duties.[17]

Levin contends that there are currently two main conceptual approaches to workplace privacy, namely, a property-focused approach and a rights-based approach.[18] Many scholars view the property-focused approach as antiquated and outmoded, though it is still the dominant model in the United States.[19] However, some commentators, such as Rasky, believe that employer ownership of workplace equipment means that employees have no expectation of privacy and, therefore, no privacy rights.[20] Others, such as Anderson, question whether the fundamental values of work and privacy can ever be reconciled.[21]

Situating the notion of privacy in the employment law context is complicated by such concepts as the division between public and private space, the contractual relationship between the employer and the employee, and the property interests of employers as the owners of the workplace. There is a

---

[16] Barbara McIsaac, Rick Shields & Kris Klein, *The Law of Privacy in Canada*, looseleaf (Scarborough: Carswell, 2000) [McIsaac] at 2.5.1.
[17] Jane Ford, "The Right to Privacy in Employment: A Management Perspective" (1991) 1 Lab. Arb. Y.B. 95 at 98.
[18] *Under the Radar*, *supra* note 14 at 3. The international aspect of these two approaches is discussed below.
[19] See e.g. Morgan, *supra* note 2 at 855; Radwanski, *supra* note 10 at 2 and 6; Marc-Alexandre Poirier, "Employer Monitoring of the Corporate E-mail System: How Much Privacy Can Employees Reasonably Expect?" (2002) 60 U.T. Fac. L. Rev. 85 [Poirier] at 96.
[20] Holly L. Rasky, "Can an Employer Search the Contents of Its Employees' E-mail?" (1998) 20 Adv. Q. 221 [Rasky].
[21] Sandra M. Anderson, "Alberta's Statutory Privacy Regime and Its Impact on the Workplace" (2006) 43 Alta. L. Rev. 647 [Anderson] at 648.

growing recognition that, due to the technological transformation of the workplace, the distinction between public and private life is very fluid, as is the distinction between "work space" and "private space".[22] In the same way, it is increasingly difficult to identify bright-line divisions between the moments when employees are "on-duty" or "off-duty".[23] As Durnford observes, some employees "have taken to living out part of their private lives at work...".[24] Lifshitz describes this as an expansion of the boundaries of the workplace:

> As the employee's workplace is expanded with the use of Blackberry®s, remote access and as individuals are working from home, on the road, and around the clock, the individual's workplace is no longer limited to the confines of the employer's place of business.[25]

The jurisprudence emanating from Quebec contains the strongest statements regarding the rights-based approach to privacy in Canada.[26] For instance, Morgan characterizes privacy as a "personality right". He elaborates:

> The very nature of a personality right is that it is held by everyone and that it cannot be alienated. It is extra-patrimonial. It is in part for this reason that it is inappropriate to suggest that ownership rights negate privacy rights. The two kinds of rights are each of a different nature; they overlap, they are not mutually exclusive.[27]

---

[22] Morgan, *supra* note 2 at 900. The unique considerations which apply to telecommuters or individuals who work from home are beyond the scope of this thesis. A separate analysis would also likely have to be done for dependent and independent contractors, though presumably they would have greater bargaining power with respect to including privacy protections in their contracts.

[23] *Ibid.* at 901.

[24] 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 [Durnford] at 65.

[25] Lisa R. Lifshitz, "Corporate Blogging: Navigating Through a Web of Potential Legal Liability – Part II of II" (2007) 7 Internet & E-Commerce Law in Canada 89 [Lifshitz, "Blogging"] at 93. See also Fernand Morin, "Nouvelles technologies et la télésubordination du salarié" (2000) 55 R.I. 725 [Morin] at 735-736.

[26] This is perhaps not surprising, given its civil law heritage, as discussed in greater detail below. On the difficulties inherent in importing civil law employment concepts into common law jurisdictions, see e.g. Debra Parkes, "Targeting Workplace Harassment in Quebec: On Exploring a New Legislative Agenda" (2004) 8 Empl. Rts. & Employ. Pol'y 423.

[27] Morgan, *supra* note 2 at 855.

Poirier confirms that "privacy rights and property rights are not mutually exclusive...privacy interests may exist in the absence of any proprietary right."[28] And further, "[i]ndividuals are entitled to a certain level of privacy in the workplace. An employee's renunciation of the right to privacy cannot be inferred from the existence of the work relationship."[29] There have been several cases in Quebec which have confirmed that an employee retains privacy rights in the workplace.[30] Quebec's civil law does not place much emphasis on the fact that the employer owns the 'tools' or technologies that the employee uses, since the civil law conceives the right to privacy as "un droit subjectif extrapatrimonial".[31]

A unique approach to workplace privacy has been advanced by Veilleux, which involves a consideration of individualistic, collectivistic and realistic approaches to workplace privacy.[32] She asserts that "[l]'approche réaliste est fondée sur la pondération entre le droit individuel à la vie privée et le droit de la société d'y accéder dans l'intérêt général."[33] She proposes a two-stage analysis for workplace privacy problems. At the first stage, the determination of whether an employee has a right to privacy is governed solely by the individualistic approach, which views the matter from the employee's perspective. It is at the

---

[28] Poirier, *supra* note 19 at 96. See also Avner Levin, "Big and Little Brother: The Potential Erosion of Workplace Privacy in Canada" (2007) 22 C.J.L.S. 197 [Levin, "Brother"] at 197, n. 4, where workplace privacy is seen as springing from workers' inherent dignity, rather than their contractual relationships with their employers.

[29] Poirier, *ibid.* at 99.

[30] See e.g. *Liberty Smelting Works (1962) Ltd. c. Syndicat international uni de l'automobile, de l'aéroneautique, de l'astronautique et des instrument aratoires d'Amérique (TUA), local 1470*, [1972] S.A.G. 1039 at 1044-1045 and *Tremblay c. La Reine*, [2003] J.Q. no 5009 (Que. C.A.), leave to appeal denied, [2003] C.S.C.R. no 233 (S.C.C.) (QL) [*Tremblay*].

[31] Karen Eltis, "La surveillance du courrier électronique en milieu de travail: le Québec succombera t-il à l'influence de l'approche américaine?" (2006) 51 McGill L.J. 475 [Eltis] at 496.

[32] Veilleux, *supra* note 13. This approach is critiqued by Levin in "Brother", *supra* note 28 at 219.

[33] Veilleux, *ibid.* at 8. The individualist and collectivist approaches are described in greater detail at 7-8 thereof.

second stage, when determining whether such rights have been waived or renounced or should be otherwise overridden, that collectivist concerns such as the rationality and proportionality of the employer's privacy-invasive conduct may be weighed in the balance.[34]

While it is difficult to distill these diverse theories of workplace privacy into a workable definition, understanding the competing property-based and rights-based approaches helps to put the emerging case law into perspective. Furthermore, a recognition that most workplace privacy disputes relate to informational privacy may assist in crafting effective legal mechanisms for their redress.

For the purposes of this thesis, a rights-based approach to workplace privacy is adopted, with an emphasis on access control. In this way, the workplace (which is not necessarily confined to a physical structure, but is inclusive of all of the places where an employee performs work-related tasks) is treated as a semiprivate zone – neither wholly public nor private – wherein employees have a right to choose whether or not to allow interference with their privacy interests and/or to disclose their personal information. This right may only be overridden by employers who demonstrate that such interference is objectively reasonable.

[34] *Ibid.* at 22 and 45.

III. Defining Electronic Employee Monitoring

Employees' privacy interests may be engaged in the workplace in a number of ways.[35] Electronic employee monitoring is one such way in which employees' privacy interests may be challenged in the workplace. As Morin explains, "[l]es technologies d'information et de communication permettent, incitent ou forcent les entreprises à modifier leurs processus de gestion et de contrôle."[36] For the purposes of this thesis, 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 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.[37]

---

[35] In "Workplace Searches and Surveillance versus the Employee's Right to Privacy" (1999) 48 U.N.B.L.J. 283 [Sherrard], Michael G. Sherrard presents a hierarchy of employee privacy rights at 298. See also deBeer, *supra* note 3 at 386-387. However, in response to deBeer's hierarchy (which includes the category of "benign surveillance"), it is questionable whether any surveillance can truly be called "benign". More sceptical critics might argue that all surveillance is somewhat menacing, as at the very least it serves to wear down the public's resistance to the notion of surveillance: see e.g. Oscapella, *supra* note 3 at 343.

[36] Morin, *supra* note 25 at 725.

[37] 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.

A number of rationales have been identified by employers and academics to support the practice of electronic employee monitoring.[38] 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 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);
- prevention or detection of unauthorized use of computer systems for criminal or terrorist activities;

Tech. L. Rev. 4 [Lasprogata] at para. 18 [emphasis added]. Throughout this thesis, the terms "monitoring" and "surveillance" are used interchangeably.

[38] 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] 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; Morgan, *supra* note 2 at 852; Uteck, *supra* note 4 at 20-21; Geist, *supra* note 5 at 155; Lauzon, *supra* note 13 at 49-50; Veilleux, *supra* note 13 at 37; Wallach, *supra* note 13 at 211; McIsaac, *supra* note 16 at 2.5.4.2; Levin, "Brother", *supra* note 28 at 217.

- 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, it is often observed that the mere possibility of employee misuse 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.[39]

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."[40] 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.

[39] As Durnford, *supra* note 24 notes at 68, "...the presence of online distractions such as Facebook are simply not reason enough for employee monitoring." See also Morin, *supra* note 25 at 740: "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."
[40] Morgan, *supra* note 2 at 901.

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:

> 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...[41]

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, one's cellphone usage and credit card activity.[42] It is the path of these digital footprints which employers trace using electronic employee monitoring techniques.

IV. Technologies Involved in Electronic Employee Monitoring

Electronic employee monitoring can take a number of forms, and the possibilities and permutations continue to increase as new technologies are developed and deployed. The following is a brief survey of the main methods for electronically monitoring employees.

---

[41] Morin, *supra* note 25 at 732. See also Levin, "Brother", *supra* note 28 at 218 and *Under the Radar*, *supra* note 14 at 3.

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

A. Audio and Video Surveillance

Audio and video surveillance are arguably the oldest forms of technologically-assisted employee monitoring. Given that the jurisprudence regarding audio and video surveillance is now fairly well-developed, it will not be reviewed extensively herein.[43] However, such cases may provide guidance and direction to decision-makers faced with employee surveillance accomplished using newer forms of technology. For instance, monitoring an employee's e-mail is sometimes analogized to recording his or her telephone calls. As telephones have been in the workplace for quite some time and limited personal use thereof has become accepted, it is argued that after internet- and e-mail-capable computers become a workplace norm, a similar trend will develop towards allowing some limited personal employee use thereof.

[43] The introduction of voice-over-internet protocol ("VoIP") "has a significant potential to diminish workplace privacy through the enhanced ability of the system to log and retain telephone conversations...": *Under the Radar*, *supra* note 14 at 11. This fusion of telephone and internet may prove to be a fruitful testing ground for older, more established concepts regarding employee privacy interests. Another interesting development is the growth of video distribution websites (such as www.youtube.com) and flourishing social networking applications (such as www.myspace.com and www.facebook.com). In this age of internet exhibitionism, it may be unnecessary for employers to spend money implementing video surveillance technology – their employees may do this job for them. Employers may simply scan these types of websites for clips or pictures regarding their employees. See e.g. "Dairy Queen workers' hijinks on web shock owner" *CBC News* (18 January 2008), online: CBC News <http://www.cbc.ca/consumer/story/2008/01/18/dairy-video.html>.

B. Computers, Internet and E-mail

As more and more employees use computers,[44] internet[45] and e-mail[46] in their work, it is perhaps not surprising that there have been instances of employee misuse of such technology. For this reason, many employers have turned to electronic methods of monitoring employees' use of workplace computers, in particular, employer-provided internet and e-mail access. Such monitoring may be accomplished in a number of ways, and may be done on either an ongoing or random basis.

There are, generally speaking, two types of computer surveillance programs, those that are server-based and those that are client-based. Server-based applications are installed on the corporate network and are usually used to monitor e-mail and internet usage. Client-based applications must be installed on individual employees' computers, but can be used to monitor non-networked activity, such as playing games or typing personal documents. These latter programs can be modified to monitor productivity, perhaps by way of keystroke

[44] Various definitions of the term "computer" were considered by the Supreme Court of Canada in *R. v. McLaughlin*, [1980] 2 S.C.R. 331. For a fuller definition, see Barry B. Sookman, *Computer, Internet and Electronic Commerce Terms: Judicial, Legislative and Technical Definitions* (Toronto: Thomson Canada Limited, 2007) [Sookman] at 69-72.

[45] The internet was described by the Supreme Court of Canada as "a huge communications facility which consists of a worldwide network of computer networks deployed to communicate information," in *Society of Composers, Authors & Music Publishers of Canada v. Canadian Association of Internet Providers*, [2004] 2 S.C.R. 427 at para. 8. In s. 127 of *The Consumer Protection Act* of Manitoba, C.C.S.M. c. C200, the "Internet" is defined as "the open and decentralized global network connecting networks of computers and similar devices to each other for the electronic exchange of information using standardized communication protocols." A fuller definition of the term is provided by Sookman, *ibid.* at 223-234.

[46] E-mail, or "electronic mail", was described by the New York Court of Appeal as a "hybrid of traditional telephone line communications and regular postal service mail," in *Lunney v. Prodigy Services Company*, 99 N.Y. Int. 0165 (Ct. App. N.Y. December 2, 1999). Further definitions of the term may be found in Sookman, *ibid.* at 158-160 and 166.

logging.[47] Common features of computer use monitoring software include customizable reports about how employees use their computers (internet activities and e-mail logs) and prevention features (such as blocking websites and filtering e-mails).[48]

Computer records are often accessed after the fact to substantiate allegations that an employee was misusing company resources and was therefore terminated for just cause. In other cases, employers may proactively install special software to track employees' computer, internet and e-mail usage, either covertly or overtly. All of these methods are forms of electronic employee monitoring.

There is a particular subset of internet usage that is worthy of special mention at this juncture, namely, the weblog or "blog". Lifshitz describes a blog as "an interactive Website where people can easily post information, opinions and pictures on an ongoing basis."[49] A corporate blog is distinguished as being "a Website published and supported by an organization or company that may serve as a marketing tool or a means to distribute timely information to the public."[50] There is even a subset of blogs that are "dedicated to complaints about work and the boss"; these websites, sometimes referred to as "gripe sites", are "websites

[47] Geist, *supra* note 5 at 160.
[48] *Ibid.* at 159-160.
[49] Lisa R. Lifshitz, "Corporate Blogging: Navigating Through a Web of Potential Legal Liability – Part I" (2007) 7 Internet & E-Commerce Law in Canada 81 at 81.
[50] *Ibid.* at 82.

or message boards where employees post personal accounts, feedback and complaints about employers, working conditions, supervisors and benefits."[51]

By their very nature, blogs pose peculiar problems for employee privacy, as they encourage exposure of intimate details with the sometimes-ephemeral promise of anonymity. Nonetheless, as discussed in greater detail below, monitoring employee blogging efforts may constitute a form of electronic employee surveillance.

C. Global Positioning Systems ("GPS")

As indicated above, privacy may be divided into three spheres: spatial/territorial, personal and informational. GPS technologies have implications for both employees' spatial/territorial and informational privacy, which might be collectively referred to as their 'locational privacy'. As Guillemette, Fontaine and Caron observed:

> One of the major characteristics of privacy protection, for individuals, is the right to move anonymously. Consequently, tracking the position of a person is considered sensitive information that directly affects privacy.[52]

Technologically speaking, GPS is a "system of satellites, computers, and receivers that is able to determine the latitude and longitude of a receiver on Earth by calculating the time difference for signals from different satellites to

---

[51] Konrad Lee, "Anti-Employer Blogging: Employee Breach of the Duty of Loyalty and the Procedure for Allowing Discovery of a Blogger's Identity Before Service of Process is Effected", online: (2006) Duke L. & Tech. Rev. 2 <http://www.law.duke.edu/journals/dltr/articles/pdf/2006dltr0002.pdf> [Lee] at para. 8.

[52] Manon G. Guillemette, Isabelle Fontaine & Claude Caron, "Hybrid RFID-GPS Real-Time Location System for Human Resources: Development, Impacts and Perspectives" (Proceedings of the 41st Hawaii International Conference on System Sciences in Waikoloa, Hawaii, January 2008) <http://csdl2.computer.org/comp/proceedings/hicss/2008/3075/00/30750406.pdf> [Guillemette] at 8.

reach the receiver."[53] GPS is often associated with "telematics".[54] While GPS was initially developed for use by the military, commercial applications of the technology now abound. While its initial uses primarily focused on navigation, particularly in remote, off-road areas, GPS is now commonly integrated into cellular telephones and automobiles and is often used by employers to monitor mobile employees. This ability to monitor mobile employees is of particular interest to employers, as such workers are generally less susceptible to traditional surveillance techniques.

D. Biometrics

Popularized by Hollywood films and science fiction novels, the use of biometrics is often linked with privacy concerns. Generally speaking, biometric information is derived from an individual's unique measurable biological characteristics.[55] As York and Carty explain:

---

[53] *The American Heritage Dictionary of the English Language*, 4th ed., *s.v.* "Global Positioning System." Similarly, the online *Oxford English Dictionary* defines "Global Positioning System" as "a worldwide navigation system which allows users to determine their location very precisely by means of receiving equipment that detects timed radio signals from a network of satellites in stable, predictable orbits…" <http://www.oed.com>.

[54] See e.g. Morin, *supra* note 25. According to "Telematics", online: Wikipedia <http://en.wikipedia.org/wiki/Telematics>:

> The term ***telematics*** is used in a number of ways:
>
> - The integrated use of telecommunications and informatics, also known as ICT (Information and Communications Technology). More specifically it is the science of sending, receiving and storing information via telecommunication devices.
> - More commonly, telematics have been applied specifically to the use of Global Positioning System technology integrated with computers and mobile communications technology in automotive navigation systems.
> - Most narrowly, the term has evolved to refer to the use of such systems within road vehicles, in which case the term **vehicle telematics** may be used.

[55] See e.g. the definition of "biometric information" provided in s. 1(b.1) of Alberta's *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25. Paragraph 1(n)(v) confirms that an individual's fingerprints or other biometric information are included in the concept of "personal information". See also *Ontario Works Act, 1997*, S.O. 1997, c. 25, Sch. A, s. 2 and *Ontario Disability Support Program Act, 1997*, S.O. 1997, c. 25, Sch. B, s. 2. A similar definition is set out

> Biometric technology uses unique physical attributes of an individual, such as a fingerprint or voice, to identify that individual. In most cases, the technology involves scanning the physical attribute, reducing it to digital form and storing it on a system so that it can be used for comparison purposes. Each time the individual wishes to gain access to the place or system protected by the biometric technology, the physical attribute is again scanned and the new scan is compared against the stored example. If the two match within a preset threshold, the individual would be granted access. Among other things, biometrics can now be used in time clocks to verify employee work hours, for security purposes in door locks, and in computer and telephone systems.[56]

Biometrics may serve either verification or identification purposes. There are both physiological and behavioural forms of biometrics. Physiological biometrics include finger scanning/geometry, hand geometry, ear geometry, facial recognition, gait recognition and iris/retinal scanning. Behavioural biometrics include voice recognition, dynamic signature verification and keystroke dynamics.[57] Both types of biometrics may be reduced to numerical form and used to identify, or verify the identity of, an individual. The monitoring of behavioural biometrics may also serve a secondary purpose, that of monitoring an employee's attitude or performance.[58]

---

in s. 5(1) of Alberta's *Electronic Transactions Act*, S.A. 2001, c. E-5.5 and Ontario's *Electronic Commerce Act, 2000*, S.O. 2000, c. 17, s. 29.

[56] Andrea York & Lisa Carty, "Biometrics in the Workplace: Balancing Technology and Privacy" (2006) 16 E.L.L.R. 21.

[57] Peter Hope-Tindall, "Biometrics 101 – An Introduction" (Paper presented in Winnipeg, 11 August 2004) [unpublished]. See also Lyne Duhaime, "La protection des renseignements personnels en milieu de travail" (November 2006), online: Fasken Martineau Dumoulin <http://www.fasken.com> [Duhaime] at 18 (where these two categories are referred to as "la biométrie morphologique ou physiologique" and "la biométrie comportementale").

[58] For instance, voice sensors may be used on workplace telephones to assess an employee's stress level: deBeer, *supra* note 3 at 387. Some digital point-of-sale machines may incorporate biometric technology: *Under the Radar*, *supra* note 14 at 11. For an indication of where such technologies may be headed in the future, see Alexi Mostrous & David Brown, "Microsoft seeks patent for office 'spy' software" *The Times* (16 January 2008), online: The Times <http://technology.timesonline.co.uk/tol/news/tech_and_web/article3193480.ece>.

E. Radio Frequency Identification ("RFID")

As with GPS, RFID may impinge upon employees' locational privacy; they have both been described as "Location Awareness Technologies".[59] As its name suggests, RFID is "a generic term for a variety of technologies that use radio waves to automatically identify individual items".[60] "Real-time Location Systems" are just one type of RFID technology.[61]

As Cavoukian explains, "[a]ll RFID systems have two integral parts: a tag, and a reader. Readers capture the information stored or gathered by the tag."[62] Originally developed for use in the Second World War, RFID has now been commercialized and is largely used for logistical purposes, such as supply chain

---

[59] Avner Levin & Mary Jo Nicholson, "Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground" (2005) 2 U.O.L.T.J. 357 at 369. See also John D. Canoni, "Location Awareness Technology and Employee Privacy Rights" (2004) 30 Employee Relations Law Journal 26 [Canoni]. Lower-tech access control systems generally involve some form of card-swiping technology, with a coded magnetic strip and a photograph of the employee: *Under the Radar*, *supra* note 14 at 11. A simpler version of "location awareness technology" that has been employed in the workplace is chair sensors, which determine how often an employee is seated at his or her desk: deBeer, *supra* note 3 at 387.

[60] Ann Cavoukian, *Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology* (February 2004), online: Office of the Information and Privacy Commissioner of Ontario <http://www.ipc.on.ca/images/Resources/up-rfid.pdf> [Cavoukian, *Tag, You're It*] at 3. A similar definition is offered by Lisa R. Lifshitz & Blair McKechnie, "RFID Technology: Current Legal and Business Considerations - Part 1" (2006) 7 Internet & E-Commerce Law in Canada 25 at 25: "The term 'RFID' has become a general term used to describe sensory technology that uses radio waves to scan and identify separate and distinct items." Further information on such systems has been compiled by the Office of the Privacy Commissioner of Canada in a fact sheet on "RFID Technology" <http://www.privcom.gc.ca/fs-fi/02_05_d_28_e.asp> and the Office's consultation paper on "Radio Frequency Identification (RFID) in the Workplace" (March 2008) <http://www.privcom.gc.ca/information/pub/rfid_e.pdf>.

[61] Guillemette, *supra* note 52 at 1.

[62] Cavoukian, *Tag, You're It*, *supra* note 60 at 4. As noted therein (at 2), RFIDs have been likened to "bar codes on steroids". This observation is based on the fact that, in a barcode system, all similar items have the same bar code (*e.g.*, a widget sold in Tokyo has the same bar code as one sold in Canada), whereas with RFIDs each individual widget has a unique identifier. In this way, specific units may be tracked with greater precision. For further information, see Teresa Scassa *et al.*, *An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies* (28 April 2005), online: Dalhousie University <http://www.library.dal.ca/law/Guides/FacultyPubs/Scassa/RFIDs_Report2(Single).pdf> and Ann Cavoukian, "RFID and Privacy: Guidance for Health Care Providers" (2008) 4 Can. Priv. L. Rev. 21.

management.[63] However, the technology's use is expanding and RFID tags or chips have been introduced into the workplace as a method for tracking the movements of employees, particularly for security and payroll purposes. 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.[64] While such a practice does not yet appear to be prevalent in Canada, it may foreshadow a potential future development on this side of the border.

F. Emerging Technologies

There are also a number of emerging technologies which may have an impact on employees' privacy. A few examples include DNA ink, invisible printer dots and memory-altering pharmaceuticals.

DNA ink can be created by taking DNA from a saliva swab, then copying it and mixing it with various proteins and enzymes:

---

[63] Cavoukian, *Tag, You're It*, *supra* note 60 at 3. The current trend of applying logistics technologies to the management of workers is an interesting phenomenon. In some ways, this could be considered to equate workers with inanimate products or goods. Some might argue that this analogy is inherently objectionable, as it devalues people and affects their dignity. In response, it could be said that this is the information age, where knowledge powers the economy. In this respect, humans are the new capital. The question remains whether they need to be tracked and managed in the same way as other goods or raw materials. This debate is exemplified in the use of biometrics, which reduce human characteristics to a set of numbers, like a human barcode.

[64] Wisconsin, North Dakota and California have all passed laws prohibiting forced RFID implantation: 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: *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: "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>.

> The system is based upon assembling small sections of DNA known as 'oligomers,' which are then encrypted in a laboratory through stringing together the As, Gs, Cs and Ts that comprise the alphabet of DNA. By scrambling the oligomer components, trillions of potential combinations can be made.[65]

The ink can be invisible and its authenticity may be verified by a small scanner.

This technology was used to prevent counterfeiting of Olympic merchandise in connection with the 2000 Summer Olympics held in Sydney, Australia. It has also been used to authenticate works of art and sports collectibles. It is possible that there will come a day when the use of such ink is commonplace and the failure of an employee to contribute his or her DNA to its production could be cause for discipline, or even dismissal.

The use of invisible printer dots has recently garnered some media attention. The technology is used by many popular laser printers and photocopiers. It works by imbedding nearly invisible tracking dots onto documents which uniquely identify the machine that printed them. While the technology was originally aimed at tracking currency counterfeiters, it has been observed that this technology could be much more widely applied.[66] For instance, in workplaces where each employee has his or her own printer, this technology could potentially be used for disciplinary purposes (*e.g.*, if an otherwise anonymous insubordinate message was printed at the office and posted on a workplace bulletin board).

---

[65] Stewart Taggart, "Call It the SyDNA Olympics" *Wired* (7 March 2000), online: Wired <http://www.wired.com/science/discoveries/news/2000/03/34774>.

[66] Dan Goodin, "Secret Printer ID Codes May Breach EU Privacy Laws" *The Register* (15 February 2008), online: The Register <http://www.theregister.co.uk/2008/02/15/secret_printer_tracking_dots>.

Lastly, scientists have been exploring the field of memory-dampening technology.[67] These memory deletion drugs could certainly play a role in the workplace of the future, particularly with respect to guarding trade secrets and other confidential, proprietary business information. However, they could also have implications for employees' privacy, including their right to protect the integrity of their memories. It is likely that occupations involving potential exposure to traumatic events will be the first to experiment with these products, such as military personnel and police officers.

While these technologies are at the early stages of development and have not yet been implemented in the workplace, they serve to illustrate that electronic employee monitoring will not always be limited to computer, internet and e-mail surveillance, or the use of GPS, biometrics and RFID. Just as audio and video surveillance have been supplemented by these newer forms of technology, this technological evolution is likely to continue. Lawyers and legal scholars must therefore be vigilant in scrutinizing the ways in which these and other new technologies are implemented in the workplace, in order to gauge their impact on employees' privacy and ascertain the appropriate legal response to such developments. Where possible, overarching technology-neutral laws relating to employee privacy issues should be implemented in advance, in order to proactively protect employees' privacy in the face of future technological developments.

[67] Cynthia Aoki, "Rewriting My Autobiography: The Legal Implications of Memory-Dampening Mechanisms" (The Student "I" Conference, delivered at the University of Ottawa Faculty of Law, 25 October 2007) [unpublished].

V. Governing Legal Framework

A. Overview of Relevant Employment Law Principles

Before an analysis of electronic employee monitoring cases can be undertaken, it is important to understand the legal framework within which such cases arise, namely, the employment relationship. Generally speaking, employees in Canada are generally subject to either an individual contract of employment enforceable in the courts or a collective agreement bargained on their behalf by a union and enforced by a grievance arbitration process. In some jurisdictions supplementary statutory unjust dismissal schemes, enforced by an adjudication procedure, have also been enacted. Employment standards legislation further supplements the law in all of these areas.[68]

This thesis is concerned with the electronic monitoring of employees in non-unionized workplaces that are not subject to statutory unjust dismissal schemes, though comparisons will be drawn to the treatment of employees in unionized workplaces and under statutory unjust dismissal schemes. There are two key sources of individual employment law, which have been referred to as its "twin pillars": the common law and employment standards legislation.[69]

The common law foundation of the employment relationship is based on the general law of contract.[70] Employment contracts do not need to be in

[68] In fact, statutory unjust dismissal regimes are often an extension of employment standards schemes: Geoffrey England, *Individual Employment Law* (Toronto: Irwin Law, 2000) [England, *Individual Employment Law*] at 291. It should be understood that these regimes are not necessarily mutually exclusive and often overlap with each other.
[69] *Ibid.* at 3.
[70] An explanation of the economic model of independent bargaining is contained in deBeer, *supra* note 3 at 406. Morin, *supra* note 25 also provides a historical and economic analysis of the employment relationship.

writing.[71] Even when they are reduced to writing, their express terms rarely cover more than the "job title, basic wage rates, basic hours of work, and possibly vacations and holidays." Occasionally, they will incorporate by reference various workplace policies, manuals or benefits handbooks.[72] As such, "[t]he flesh and blood of the employment contract...normally consists of implied terms."[73] England explains the process of implying terms in the following manner:

> The process of implying terms into an employment contract is supposed to be that courts will give effect only to the unexpressed intentions of the parties regarding the matter in issue. This is supposed to ensure that freedom of contract is respected. Thus, a longstanding and certain past practice that is known to both parties may be implied into the employment contract as reflecting their common unstated [p. 28] intention. ... Clearly, if one side either does not know of the custom or practice, or expressly objects to having it applied to him or her, the custom or practice cannot be impliedly incorporated as a term of the contract.[74]

While the focus is generally on implied terms which govern the conduct of employees, particularly in the context of wrongful dismissal actions, another important implied term in the employment relationship is the employer's ability to control the workplace and direct its employees.[75] In the civil law context, articles 2085 and 2088 of the *Civil Code of Québec* confirm "le droit de direction de

---

[71] England, *Individual Employment Law*, *supra* note 68 at 26.
[72] *Ibid.* at 27.
[73] *Ibid.* See also Geoffrey England & Roderick Wood, *Employment Law in Canada*, 4th ed., looseleaf (Markham: LexisNexis Butterworths, 2005) [England & Wood] at §1.16: "the standard implied terms will represent the norm for most workers, notwithstanding that, technically speaking, they form the default position in the absence of express contractual terms on the matters in question."
[74] England, *Individual Employment Law*, *supra* note 68 at 27-28. One such implied term is a duty of fairness on the part of the employer. While this implied term is still nascent, *quaere* whether, if the law on this point continues to expand, it might extend to respecting employee privacy interests.
[75] Klein, *supra* note 38 at 135. See also Rasky, *supra* note 20 at 221.

l'employeur."[76] However, Morgan argues that this right is limited, as it must be tied to the purpose of the employment contract; as such, "employer directives and surveillance must be effected in direct relation to the carrying out of obligations as set forth in the contract of employment."[77]

At common law, the employment relationship may only be terminated upon reasonable notice, unless the employer has just cause for dismissing the employee. As Lifshitz explains:

> ...[T]here is no need for an employer to give notice of termination where the employer has cause to dismiss an employee. This may occur when the employee breaches one of the implied duties to the employer: to obey, to exercise skill and care, or good faith or fidelity. 'Just cause' for dismissal also includes: dishonesty, revelation of character, insolence and insubordination, disobedience, lateness and absenteeism, incompetence, improper conduct outside the workplace, permanent illness or disability, disruption of corporate culture, alcohol and drug abuse, conflict of interest, or sexual harassment.[78]

It should also be noted that "[g]rounds for dismissal do not have to be shown at the time of the dismissal, provided they can be subsequently established."[79] The determination of whether cause exists was described as follows in *Foerderer* at para. 151:

> Cause is determined by an objective contextual and proportional analysis. A finding of misconduct does not, by itself, give rise to just cause; the question is whether, in the circumstances, the behaviour is such that the employment relationship could no longer viably subsist. There must be a balance struck between the severity of an employee's misconduct and the sanction imposed. The factors

[76] Veilleux, *supra* note 13 at 37.
[77] Morgan, *supra* note 2 at 888-889.
[78] Lifshitz, "Blogging", *supra* note 25 at 92.
[79] *Foerderer v. Nova Chemicals Corp.*, 2007 ABQB 349 [*Foerderer*] at para. 63. This is tied to the third branch of the Lasprogata definition of electronic employee monitoring quoted above (*supra* note 37). See e.g. *Manchulenko v. Hunterline Trucking Ltd*., 2002 BCSC 966 [*Manchulenko*].

> considered include the employee's tenure, employment record, and the seriousness of the misconduct.

Not every act of employee misconduct will provide just cause for dismissal; "[w]hether an employer is obliged to provide an employee with a clear and unequivocal warning and opportunity to improve depends on the circumstances and the quality of the misconduct."[80] This is the doctrine of progressive discipline. Where employees' misconduct is not so serious as to irrevocably damage the trust foundation of the employment relationship, they may still be discharged for repeated minor breaches of the employment contract (including their implied duties) if they have been adequately warned and given the opportunity to correct their behaviour. As Ball observes, "[n]eglect of duty by the employee following repeated warnings by an employer may constitute wilful neglect of duty and can amount to sufficient cause to justify summary dismissal."[81]

A key concept related to this point is the doctrine of condonation. As Ball explains:

> The atmosphere at the workplace may lead an employee to conclude that a certain conduct will not place his or her job in jeopardy, hence, that the conduct is condoned by the employer. When the employer permits other employees to engage in a particular conduct, the court will be inclined to consider the employer to have condoned similar conduct being carried on by the plaintiff.[82]

---

[80] *Foerderer*, *ibid.*

[81] Stacey Reginald Ball, *Canadian Employment Law*, looseleaf (Aurora: Canada Law Book, 1996) [Ball] at 11:130.

[82] *Ibid.* at 11:80. Or, as Poirier succinctly states (*supra* note 19 at 103), "the negligent or non-uniform application of a policy may nullify the effect that it otherwise could have had on an employee['s] privacy expectations." While employers have the onus of proving just cause for dismissal, employees must prove condonation: see e.g. *Foerderer*, para. 63.

Thus, employers concerned about being deemed to have condoned certain employee misconduct may engage in monitoring to ensure that workplace policies, such as computer usage policies, are consistently enforced.[83] In this way, it appears that the current state of the law encourages and perpetuates electronic employee monitoring, as only policies that are consistently and vigilantly enforced can be relied upon in termination disputes.

There are two fundamental problems with what has been termed the "contractualist approach" to the employment relationship.[84] First, due to its contract law foundation, it assumes that the employer and the employee have freely negotiated the terms of employment in an open market. However, this legal fiction ignores the fact that, in most cases, the employment relationship is characterized by an imbalance of power, with employers dictating employees' working conditions. The second problem relates to enforcement, and the often prohibitively expensive nature of litigation. This explains why most reported cases involve senior employees or professionals. The purpose of employment standards legislation is to remedy this imbalance of power and provide a cost-effective means for employees who cannot afford to litigate to enforce their rights.[85]

A further difficulty with the contract law theory of employment law in relation to employee privacy issues is whether employee privacy is a good that is

---

[83] Max Brunette, "Caught With Their Virtual Pants Down: Can Sending, Receiving and Procuring Offensive Materials from a Workplace Computer Constitute Dismissal for Just Cause?" (2007) 17 E.L.L.R. 69 [Brunette] at 72. Lauzon observes that in cases involving electronic employee monitoring, employees' two main defences are (1) violation of privacy and (2) condonation by the employer or a lack of clearly established rules: *supra* note 13 at 52.
[84] England, *Individual Employment Law*, *supra* note 68 at 350-351.
[85] *Ibid.* at 3. See also 6 and England & Wood, *supra* note 73 at §1.20.

capable of commoditization. As well, the contract law theory falls short with respect to surreptitious surveillance, as "employees cannot bargain with respect to invasions that they are unaware of."[86]

Employment standards legislation establishes what is commonly referred to as a 'floor of rights', because "the benefits they provide cannot be reduced by private bargaining in the individual employment contract, but can only be enlarged upon."[87] Such legislation was "inspired by the general movement to advance individual 'rights' in all walks of life, which has dominated Canadian political culture during most of the post-war period."[88] England and Wood's text offers the following definition of this "rights" paradigm:

> ...[I]ts essence is that the individual employee has certain inalienable 'fundamental human rights' that must be guaranteed in the workplace in order for our system of work organization to be considered morally 'just' and, therefore, worthy of support. Most proponents of this paradigm would probably agree that, at the least, it requires superior power wielders to exercise their authority with due regard for the personal dignity and autonomy of those who are affected by their decisions.[89]

However, most employment standards statutes do not currently contain any provisions regarding employee privacy.[90] Some scholars, such as England and Wood, predict that "[m]odern human rights legislation has, and will likely

---

[86] deBeer, *supra* note 3 at 407.
[87] England, *Individual Employment Law*, *supra* note 68 at 5. Broadly speaking, employment standards legislation includes, *inter alia*, labour standards, pay equity, occupational health and safety, pension benefits and human rights: *ibid.* at 351.
[88] *Ibid.* at 351. This movement has been called the "rights revolution": Michael Ignatieff, *The Rights Revolution* (Toronto: House of Anansi Press, 2000).
[89] England & Wood, *supra* note 73 at §1.22.
[90] England, *Individual Employment Law*, *supra* note 68 at 139. See also England & Wood, *supra* note 73 at §8.282; Levin, "Brother", *supra* note 28 at 199; *Under the Radar*, *supra* note 14 at 4; Yves Saint-André, "Le respect du droit à la vie privée au travail: mythe ou réalité?" in *Développements récents en droit du travail*, Vol. 205 (Cowansville: Les Éditions Yvon Blais Inc., 2004) 51 [Saint-André] at 55.

continue to fuel the expectation of Canadian workers for more 'rights'."[91] This may eventually extend to privacy rights, including restrictions on electronic employee monitoring.

B. Sources of Privacy Law in Canada

As Morgan aptly observed, "[t]here is no single 'privacy law' that treats the issue of privacy protection in the Canadian workplace."[92] Despite a myriad of overlapping privacy laws, in provinces without private sector privacy legislation it has been said that, "[u]nder current Canadian law, employee surveillance in the private sector remains virtually unregulated."[93]

An additional layer of complexity is added by the constitutional division of powers between the federal and provincial levels of government.[94] Perhaps not surprisingly, neither the federal nor the provincial governments were expressly granted jurisdiction over privacy matters by the Canadian constitution. As McIsaac explains:

> Normally, that would result in the provinces having responsibility and jurisdiction. However, the transborder or interprovincial and international nature of the problem invokes federal jurisdiction as well. Privacy is one of those matters where there is clearly overlapping federal and provincial jurisdiction depending on the context and the circumstances in which the issue arises. …

---

[91] England & Wood, *supra* note 73 at §1.25.
[92] Morgan, *supra* note 2 at 872. See also Klein, *supra* note 38 at 1.
[93] Klein, *ibid.* at 56. See also McIsaac, *supra* note 16 at 2.5.4.3(b) and Levin, "Brother", *supra* note 28 at 217. It should be noted that in this thesis the provisions of the various legislative regimes are merely described as they appear on their face; the protections they provide to employees may be lessened by the manner in which they are enforced. See e.g. Office of the Privacy Commissioner of Canada, News Release, "Lack of basic privacy and security measures causing major data breaches, Privacy Commissioner says" (3 June 2008), online: OPC <http://www.privcom.gc.ca/media/nr-c/2008/nr-c_080603_e.asp>.
[94] *Constitution Act, 1867* (U.K.), 30 & 31 Vict., c. 3, reprinted in R.S.C. 1985, App. II, No. 5, ss. 91 and 92.

> Similarly, the provincial governments can legislate in respect of the collection, retention and use of personal information by employers about their employees, provided that the employment itself is subject to provincial regulation. The federal government, on the other hand, can provide similar regulation in the federally regulated employment context.[95]

It is due to these constitutional constraints that the current Canadian approach to workplace privacy is fairly fragmented and somewhat incongruous.

1. Canadian Charter of Rights and Freedoms

The *Canadian Charter of Rights and Freedoms* (the "Charter") forms part of the Canadian constitution and enshrines a variety of rights that individuals can claim vis-à-vis the government.[96] Section 8 thereof guarantees that "[e]veryone has the right to be secure against unreasonable search or seizure." This has been held to include a right to privacy.[97] As Mr. Justice Binnie observed in *R. v. Tessling*, "the Court early on established a purposive approach to s. 8 in which privacy became the dominant organizing principle."[98] In fact, "[p]rior to the introduction of the [Charter] in Canada, privacy rights were afforded little weight."[99] Interestingly, much of the development of this right may be attributed to the writings of Mr. Justice La Forest. For instance, in *R. v. Dyment*, he wrote:

> Grounded in man's physical and moral autonomy, privacy is essential for the well being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order. The restraints imposed on

---

[95] McIsaac, *supra* note 16 at 1.5.1.
[96] 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. As a general rule, the Charter does not apply to disputes between private parties, such as a private sector employer and one of its employees.
[97] As an early example of the jurisprudence, see *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, especially at 159. For a more recent summary of the pertinent case law, see *R. v. Sharpe*, [2001] 1 S.C.R. 45 at para. 26, McLachlin C.J.C.
[98] *Supra* note 15 at para. 19.
[99] Morgan, *supra* note 2 at 862.

> government to pry into the lives of the citizen go to the essence of a democratic state.[100]

Two years later, in *R. v. Duarte*, Mr. Justice La Forest observed that "as a general proposition, surreptitious electronic surveillance of the individual by an agency of the state constitutes an unreasonable search or seizure under s. 8 of the *Charter*."[101] In particular, he stated that "one can scarcely imagine a state activity more dangerous to individual privacy than electronic surveillance…."[102] And further:

> The reason for this protection is the realization that if the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful residuum to our right to live our lives free from surveillance. The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private. A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning.[103]

Later in the same year, Mr. Justice La Forest authored another decision with respect to privacy rights. In *Thomson Newspapers Ltd. v. Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)*, he wrote:

> The ultimate justification for a constitutional guarantee of the right to privacy is our belief, consistent with so many of our legal and political traditions, that it is for the individual to determine the manner in which he or she will order his or her private life.[104]

---

[100] *Supra* note 15 at para. 17.
[101] [1990] 1 S.C.R. 30 at 42.
[102] At 43.
[103] At 44. Later on, at 51, he remarked that "Surreptitious electronic recording annihilates the very important right to determine to whom we speak, *i.e.*, the right to choose the range of our auditors." And, at 53: "this freedom not to be compelled to share our confidences with others is the very hallmark of a free society."
[104] [1990] 1 S.C.R. 425 at 517.

However, he went on to find that individuals do not normally have a very high expectation of privacy in business records, as they "do not normally contain information about one's lifestyle, intimate relations or political or religious opinions."[105] Nevertheless, he did recognize that "[p]eople who work in offices...[p. 522] think of their own offices as personal space in a manner somewhat akin to the way in which they view their homes, and act accordingly."[106] He further confirmed that "human life is not divisible into mutually exclusive compartments of professional and personal which correspond with the office and the home."[107] He held that extending searches beyond business records to "indicators of the personal life" of those working in the office would seriously invade their right to be secure against unreasonable search and seizure.[108]

These cases demonstrate that fundamental notions of privacy underlie the guarantee included in section 8 of the Charter. And, as the Charter pertains to government action, government employees may claim its protection:

> As a result, government monitoring policies must strike a balance between individuals' 'expectations of privacy' and the government's 'duty to protect sensitive information and government assets (including computers and networks), and to ensure that the government conducts its activities efficiently and in conformity with law.'[109]

---

[105] At 517.
[106] At 521-522.
[107] At 522.
[108] At 522. In the later case of *R. v. Plant*, [1993] 3 S.C.R. 281, Mr. Justice Sopinka confirmed that privacy and property interests do not necessarily coincide and that ownership is not determinative in the reasonable expectations analysis required by s. 8 (at 291-292).
[109] Jeffrey Sack *et al.*, eds., "Governments Move to Limit Employees' Internet Access and E-mail Use" (November/December 2000) 24 *Collective Bargaining Reporter*.

Some commentators have queried whether section 8 of the Charter will become "another potential shield against the surveillance of employees."[110] It seems as though this may be so, at least for employees of organizations governed by the Charter. However, while reliance on *Charter* values may be helpful to employees who wish to protect their privacy, a survey of the case law in this area indicates that courts have not been very receptive to such arguments in cases involving non-governmental employees, particularly in the non-union context. As deBeer notes, "[r]arely, if ever, have *Charter* values been invoked with respect to an individual employment privacy dispute."[111]

2. Criminal Code

The *Criminal Code* of Canada contains several provisions regarding electronic monitoring – specifically, the interception of communications.[112] However, these provisions do not generally apply in the workplace, as employees either expressly or impliedly consent to monitoring or they are not found to have a reasonable expectation of privacy in the circumstances.[113] As deBeer observes, these provisions do not provide much, if any, protection to employees with respect to electronic monitoring by their employers.[114]

---

[110] E.B. Willis & W.K. Winkler, *Labour Arbitration: The Year in Review 2006* (Aurora: Canada Law Book, 2007) at 39.
[111] deBeer, *supra* note 3 at 405. See also 404. As deBeer observes, Charter arguments have found more fertile soil in the arbitration context. Uteck is of the view that "The *Charter* and the *Criminal Code* do not represent viable alternatives for the private sector employee": Uteck, *supra* note 4 at 156.
[112] R.S.C. 1985, c. C-46, ss. 184 and 342.1(1)(b).
[113] Klein, *supra* note 38 at 57.
[114] deBeer, *supra* note 3 at 394-395.

3. Public Sector

Public sector privacy laws have existed in Canada much longer than their private sector counterparts and have been enacted in every Canadian jurisdiction.[115] While public sector privacy laws are largely aimed at protecting the privacy of citizens vis-à-vis their government, they also usually apply to public sector employees. As Klein and Gates explain, at the federal level:

> The federal *Privacy Act* of 1982 regulates the collection, use and disclosure of personal information by federal government institutions, including government employers, and controls the rights of individuals to access personal information held by those agencies.[116]

While not necessarily relevant to the issue of electronic employee monitoring, it should also be noted that several provinces have passed legislation regarding the privacy of personal health information.[117] In some circumstances, this legislation may also apply to employees' personal health information.

---

[115] *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*, *supra* note 55; *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*, C.C.S.M. c. F175; *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.

[116] Klein, *supra* note 38 at 2.

[117] *Health Information Act*, R.S.A. 2000, c. H-5; *Health Information Protection Act*, S.S. 1999, c. H-0.021; *The Personal Health Information Act*, S.M. 1997, c. 51; *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, Sch. A.

4. Private Sector

(a) Federal

The *Personal Information Protection and Electronic Documents Act* ("PIPEDA") came into effect on January 1, 2001.[118] It regulates how private sector organizations collect, use, retain and disclose personal information in the course of their commercial activities. It also applies to personal information about employees of federal works, undertakings and businesses.[119] The term "personal information" is defined to mean "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization".[120] Thus, "an image captured by a video camera, a personal e-mail sent to a friend, a telephone conversation with a family member, or the location of a worker at any given time during work...are all examples of personal information."[121]

While PIPEDA is primarily concerned with consent, from an employee's perspective perhaps the most important provision in PIPEDA is the additional requirement that organizations only collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the

---

[118] S.C. 2000, c. 5. It should be noted that the Quebec government has challenged the constitutionality of PIPEDA. 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.

[119] PIPEDA, s. 4(1)(b). The phrase "federal work, undertaking or business" is defined in s. 2(1). See generally Klein, *supra* note 38 at 3-4.

[120] PIPEDA, s. 2(1). See also deBeer, *supra* note 3 at 410. However, it has been held that PIPEDA does not extend to situations of attempted collection: see *Morgan v. Alta Flights (Charters) Inc.*, 2006 FCA 121.

[121] Levin, "Brother", *supra* note 28 at 200, n. 13.

circumstances.[122] This objective reasonableness component helps counteract the difficulties that an entirely consent-based model would present in the employment context, due to the aforementioned imbalance of power inherent in the employment relationship.[123]

As deBeer observes, the above-described "constitutional constraints...preclude the application of federal legislation to employees within the provinces".[124] PIPEDA "expressly includes only employees of federal works, and by implication, excludes employees of non-federal works" because of "the limited scope of the federal power to regulate trade and commerce".[125] And further:

> Thus, it seems that [PIPEDA] would only apply when employees' information itself is the subject of a commercial transaction, or is somehow disclosed outside of the employment relationship. Thus, [PIPEDA] does not govern employment matters, other than in the federal context.[126]

Nevertheless, deBeer believes that PIPEDA can still significantly 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, [PIPEDA] ceases to apply in that

---

[122] PIPEDA, s. 5(3). See generally Durnford, *supra* note 24 at 66.
[123] Geist, *supra* note 5 at 170. See also 154. Of course, the same might be said about the consumer-corporation relationship, which is PIPEDA's primary target. LaBossiere, Clearwater and Hoeppner posit that "the common thread tying all privacy issues together is the requirement that any actions of collection, use or disclosure of personal and private information must be governed by a standard of reasonableness": Keith D. LaBossiere, Karen Clearwater & Scott Hoeppner, "The Nuts and Bolts of Accommodating Employee Privacy" (2007) Pitblado Lect. [LaBossiere] at 21. However, it might be argued that this statement only relates to the informational privacy sphere.
[124] deBeer, *supra* note 3 at 408.
[125] *Ibid.* at 397.
[126] *Ibid.*

> province. Thus, [PIPEDA] sets minimum requirements and encourages provinces to meet or exceed those standards.[127]

In terms of legislative drafting techniques, PIPEDA's structure is rather unusual. Its privacy provisions are split between the body of the legislation and three accompanying schedules. This is because PIPEDA grew out of prior voluntary efforts to regulate personal information in the private sector. As Spaeth observes, "[m]uch of PIPEDA is based upon [the] ten privacy principles originally set forth in the Canadian Standards Association ('CSA') Model Code for the Protection of Personal Information."[128] Schedule 1 of PIPEDA is actually the "Principles Set Out in the National Standard of Canada Entitled *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96". Thus, "the principles of the CSA's Model Code were ultimate incorporated (with modifications) into PIPEDA."[129] It should be noted that PIPEDA is currently undergoing its first mandatory Parliamentary review, so it is likely that changes will be made to the legislation in the near future.[130]

As indicated above, the "rights paradigm" has come to dominate the Canadian approach to employment law, particularly with respect to the statutory

---

[127] *Ibid.* at 408. See also PIPEDA, s. 26(2)(b).

[128] Juliana M. Spaeth, Mark J. Plotkin & Sandra C. Sheets, "Privacy, Eh!: The Impact of Canada's *Personal Information Protection and Electronic Documents Act* on Transnational Business" (2002) 4 Vand. J. Ent. L. & Prac. 28 [Spaeth] at 32. See also *Eastmond v. Canadian Pacific Railway*, 2004 FC 852 [*Eastmond*] at paras. 20-22.

[129] Spaeth, *ibid.*

[130] Such reviews are mandated by PIPEDA, s. 29(1). At the time of writing, the committee reviewing the legislation had issued its report (http://cmte.parl.gc.ca/cmte/CommitteePublication.aspx?COM=10473&Lang=1&SourceId=204322), the government had prepared its response (http://www.ic.gc.ca/epic/site/ic1.nsf/en/00317e.html) and it had received a number of submissions (http://www.ic.gc.ca/epic/site/ecic-ceac.nsf/en/gv00428e.html). In particular, the government agreed with the committee's recommendation that amendments be introduced to PIPEDA to address the unique privacy issues relating to the employment relationship.

protections provided to employees. PIPEDA is simply another example of the continuation of this trend. As Anderson observes:

> The privacy statutes are stark indicators of our 'rights' culture, where individuals expect to be able to protect themselves against intrusive actions from others and to be given the legal tools to do so. They remind us that the collective activities of the workplace no longer dominate our culture. The production and manufacturing of 'real' goods is yielding ground to information technology as the work product of our age. In such an environment, privacy concerns are likely to consume an ever larger proportion of workplace energy and focus.[131]

There are two easily discernible currents running through the existing legal scholarship on the topic of workplace privacy. One group of commentators believes that workplace privacy disputes may be resolved by examining, managing or even manipulating the reasonable expectations of employees.[132] The other group argues that it is employers' actions that must be subjected to scrutiny, by being measured against an objective standard of reasonableness.[133] This latter group hails the passage of PIPEDA and substantially similar provincial private sector privacy legislation as a triumph of their school of thought over the older, American-style approach based on employees' reasonable expectations.[134]

The key policy question underlying this debate is whether the role of the law is merely to protect existing expectations (*i.e.*, those that have not already

---

[131] Anderson, *supra* note 21 at 680.
[132] See e.g. *ibid.* at 679; Rasky, *supra* note 20 at 222; Lifshitz, "Blogging", *supra* note 25.
[133] See e.g. Geist, *supra* note 5 at 188; Morgan, *supra* note 2 at 855; Murray Long, "The Challenge of Employment Consent Under PIPEDA" (2006) 3 Can. Privacy L. Rev. 49 [Long]; LaBossiere, *supra* note 123; Durnford, *supra* note 24; Poirier, *supra* note 19; Radwanski, *supra* note 10 at 6; and Levin, "Brother", *supra* note 28.
[134] It should be remembered that s. 8 of the Charter only protects reasonable expectations of privacy, so cases decided under that rubric may have only limited application to regimes that rely on an objective reasonableness standard, such as PIPEDA.

been extinguished) or to create a reasonable expectation of privacy even though none presently exists. The question that must be answered is whether individual waivers of reasonable expectations of privacy should reign supreme, or whether the law should create a floor of rights with respect to reasonable expectations of privacy in the workplace out of which employers and employees cannot contract.

(b) Provincial

Three provinces have enacted private sector privacy legislation that is substantially similar to PIPEDA, namely, British Columbia, Alberta and Quebec.[135] As such, "[m]ost Canadian provinces do not have comprehensive legislated safeguards for the privacy of employees in the private sector."[136]

---

[135] *Personal Information Protection Act*, S.B.C. 2003, c. 63 [BC PIPA]; *Personal Information Protection Act*, S.A. 2003, c. P-6.5 [AB PIPA]; *An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-39.1. Ontario's health privacy legislation, *supra* note 117, has also been recognized as substantially similar to PIPEDA, but it is not relevant for the purposes of this paper. Substantially similar private sector privacy legislation has been proposed in Manitoba, in the form of a private member's bill, but has not been passed into law: Bill 216, *The Personal Information Protection and Identity Theft Prevention Act*, 2nd Sess., 39th Leg., 2007. Manitoba does, however, have some legislative protections regarding personal information in the employment context: *The Personal Investigations Act*, R.S.M. 1987, c. P34. Legislation that was substantially similar to PIPEDA was drafted in Ontario, but was never introduced: see generally Andrea York & Bonny Miller, "Privacy in the Ontario Workplace: A Review of the Draft *Privacy of Personal Information Act, 2002*" (2002) 12 E.L.L.R. 25. This has not deterred the Ontario Information and Privacy Commissioner from issuing numerous guidelines regarding workplace privacy matters. See e.g. "Workplace Privacy: A Consultation Paper" (http://www.ipc.on.ca/images/Resources/wpp-e.pdf); "Workplace Privacy: The Need for a Safety Net" (http://www.ipc.on.ca/images/Resources/safnet-e.pdf); "Privacy Protection Principles for Electronic Mail Systems" (http://www.ipc.on.ca/images/Resources/email-e.pdf); "Privacy Protection Principles for Voice Mail Systems" (http://www.ipc.on.ca/images/Resources/up-1vmail_e.pdf); "Safeguarding Privacy in a Mobile Workplace: Protect the Information You Keep on Your Laptops, Cellphones and PDAs" (http://www.ipc.on.ca/images/Resources/up-mobilewkplace.pdf).

[136] England & Wood, *supra* note 73 at §8.272.

(i) British Columbia and Alberta

Unlike PIPEDA, British Columbia and Alberta's legislation contains a special regime for addressing personal employee information.[137] These statutes expressly recognize that a consent-based approach to personal information in the employment relationship is unrealistic. Instead, they combine an objective reasonableness requirement with a more notice-based approach. As Anderson describes,

> [The legislation] permits an employer to collect, use and disclose [personal employee] information without the employee's consent so long as the purpose for collecting, using or disclosing is explained, notice is given, and reasonable opportunity to refuse consent is afforded the employee.[138]

Long agrees that, in the employment context, "[r]ather than a consent necessity, it may be far better to rely entirely on a rigorous application of the reasonable person standard for purposes."[139] Given the potential artificiality of consent in the context of the employment relationship, this reasoning seems sound.

Levin has noted that most of the workplace privacy decisions rendered by the British Columbia and Alberta privacy commissioners "surround circumstances of discipline which have led the disciplined employee to seek the aid of the privacy commissioner in releasing or suppressing records...related to the events that prompted the disciplinary action."[140] He also suggests that privacy commissioners often apply labour-based workplace privacy concepts in individual

---

[137] For an overview of this legislation and a review of recent cases of interest, see Eleni Kassaris, "Employee Personal Information: A Review of Recent Privacy Law Decisions in British Columbia and Alberta" (2007) 17 E.L.L.R. 1.
[138] Anderson, *supra* note 21 at 654. See also Levin, "Brother", *supra* note 28 at 204.
[139] Long, *supra* note 133 at 53. He argues that PIPEDA should be amended to adopt a similar approach to employee privacy for federal works, undertakings and businesses.
[140] Levin, "Brother", *supra* note 28 at 210.

employment cases, resulting in a transplantation of legal principles between what are often viewed as 'separate silos' of law.[141]

Given the lack of substantially similar private sector privacy legislation in other provinces, "BC and Alberta's legislation has become the *de facto* standard for the national employers with respect to workplace privacy simply for reasons of compliance."[142] In deBeer's opinion, "[t]he only tenable solution is for each province to enact laws that address privacy in the employment context, using [PIPEDA] as a template."[143] Whether such legislation ever materializes – and, if so, whether it takes the form of stand-alone private sector privacy legislation or an amendment to existing employment standards – remains to be seen.

As with PIPEDA, both British Columbia and Alberta's private sector privacy statutes contain provisions mandating legislative review within a particular time frame.[144] A review of the Alberta legislation was undertaken in 2006-2007.[145] A review of British Columbia's legislation was completed earlier in 2008.[146]

(ii) Quebec

Quebec has always been Canada's privacy leader. It enacted private sector privacy legislation years before PIPEDA and its provincial counterparts.[147]

---

[141] *Ibid.*
[142] *Under the Radar*, *supra* note 14 at 18.
[143] deBeer, *supra* note 3 at 383. See also 409 and 417. Uteck, *supra* note 4 reached the same conclusion (at 189-190).
[144] AB PIPA, s. 63; BC PIPA, s. 59.
[145] The committee's report is available online at http://www.assembly.ab.ca/committees/reports/PIPA/finalpipawReport111407.pdf.
[146] The committee's report is available online at http://www.leg.bc.ca/cmt/38thparl/session-4/pipa/reports/PDF/Rpt-PIPA-38-4-2008-APR-17.pdf.
[147] Its legislation was passed in 1994. Like PIPEDA, and unlike the AB and BC PIPAs, it does not contain any different or special provisions with respect to privacy in the workplace: see e.g. Levin,

Quebec's civil law tradition greatly influences its treatment of privacy.[148] Whereas other privacy legislation in Canada is concerned reasonableness in the protection of personal information, the protection of privacy in Quebec is tied to notions of individuals' inherent dignity.[149] As Eltis explains:

> D'autre part, le droit à la vie privée dans les pays de droit civil est réputé être un droit extrapatrimonial, relié à la personnalité et non à la propriété. En fait, il s'agit d'un droit inaliénable, ayant trait à l'autonomie morale et à la dignité. La dignité, pour sa part, est couronnée la valeur primordiale dans la hiérarchie des valeurs de plusieurs constitutions de pays civilistes.[150]

It should also be noted that the right protected in Quebec is slightly different than that protected elsewhere in Canada; Quebec's laws refer to "la droit à la vie privée", that is, a right to private life, which is arguably different from a right to privacy.[151] For instance, under section 5 of the Quebec *Charter of Human Rights and Freedoms* (the "Quebec Charter"), every person has a right to respect for his or her private life.[152] Thus, it is incongruous to speak of a 'reasonable expectation of privacy' in Quebec, because the right to privacy is inalienable – even in the workplace.[153]

Another relevant provision of the Quebec Charter is article 46, which states that an employer must offer its employees just and reasonable working

---

"Brother", *supra* note 28 at 202; Karl Delwaide & Antoine Aylwin, *Learning from a Decade of Experience: Quebec's Privacy Sector Privacy Act* (Ottawa: Privacy Commissioner of Canada, 2005) at 10; *Under the Radar*, *supra* note 14 at 5.

[148] Eltis argues (*supra* note 31 at 489) that Quebec's civil law tradition is better suited to handling workplace privacy disputes than the common law. As she says at 490, in Quebec law, "la dignité survit au contrat de travail".

[149] Levin, "Brother", *supra* note 28 at 203.

[150] Eltis, *supra* note 31 at 489.

[151] *Ibid*. at 501. See also Veilleux, *supra* note 13.

[152] R.S.Q., c. C-12. Perhaps the most well-known case regarding this provision is the Supreme Court of Canada's decision in *Aubry v. Éditions Vice-Versa*, [1998] 1 S.C.R. 591 which held, *inter alia*, that "une personne peut se trouver en public et prétendre néanmoins à un espace de vie privée": Veilleux, *supra* note 13 at 8.

[153] Eltis, *supra* note 31 at 502. See e.g. *Tremblay c. La Reine*, *supra* note 30.

conditions. As Eltis explains, because of this provision, “le contrat de travail comporte une obligation quasi-constitutionelle de respecter la dignité des salariés.”[154] Quebec’s Charter enjoys quasi-constitutional status. As well, unlike the Canadian Charter, the Quebec Charter applies to all disputes, whether or not they involve government action.[155]

In addition, article 35 of the *Civil Code of Québec* provides that every person has a right to the respect of his or her reputation and privacy; “[n]o one may invade the privacy of a person without the consent of the person or his heirs unless authorized by law.”[156] Article 36 provides further protections regarding the interception and use of personal communications.[157]

Quebec’s private sector privacy legislation must be read in conjunction with these more fundamental provisions. This is an example of how public law infiltrates and influences the private sphere in that province.[158] In sum, “employers in Quebec are prevented from conducting workplace surveillance for a purpose, or in a manner, that does not respect their workers’ dignity.”[159] As Saint-André concludes, “une surveillance électronique continue et systématique des salariés est susceptible d’être [p. 68] considérée comme une atteinte au droit à la vie privée ainsi qu’une condition de travail injuste et déraisonnable au sens de l’article 46 de la Charte.”[160]

---

[154] Eltis, *ibid.* at 491.
[155] Morgan, *supra* note 2 at 885. See e.g. *Laval (Société de transport de la Ville de) c. X*, [2003] C.A.I. 667, discussed in Levin, “Brother”, *supra* note 28 at 214. For a comparison of the two Charters, see Veilleux, *supra* note 13 at 9.
[156] Morgan, *ibid.* at 886.
[157] *Ibid*.
[158] Eltis, *supra* note 31 at 492.
[159] Levin, “Brother”, *supra* note 28 at 202-203.
[160] Saint-André, *supra* note 90 at 67-68.

5. Statutory Torts

In addition to the aforementioned private sector privacy laws, several provinces have created statutory torts pertaining to the invasion of privacy. Such legislation exists in four of Canada's common law provinces, namely, British Columbia, Manitoba, Newfoundland and Labrador and Saskatchewan.[161]

In brief, this legislation generally creates a tort of violation or invasion of privacy. It may give examples of what types of conduct constitute invasions of privacy for the purposes of the statute. It generally addresses the issue of remedies, including the relevant considerations in awarding damages. It also contains a variety of defences, such as consent or lawful authority.

Unfortunately, these statutes have not been widely applied, in workplace matters or otherwise. This is likely due, at least in part, to their private enforcement mechanisms and the ever-increasing cost of litigation. As well, these statutes are not well-suited to application in the employment context, as they contain broad consent defences. Unlike PIPEDA or its provincial counterparts, there is no overriding reasonableness requirement; consent is a complete defence. In addition, it is questionable whether monetary damages are adequate compensation for violations of employees' privacy.[162]

6. Common Law

While the common law is often praised for its ability to adapt to changing circumstances and social realities, to date the common law of privacy has not

---

[161] *Privacy Act*, R.S.B.C. 1996, c. 373; *The Privacy Act*, R.S.M. 1987, c. P125; *Privacy Act*, R.S.N. 1990, c. P-22; *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>.

[162] deBeer, *supra* note 3 at 400. See also Levin, "Brother", *supra* note 28 at 205-206.

developed to a point where it can be relied upon to assist individual employees with respect to electronic monitoring by employers. Just over ten years ago, Lord Hoffman stated that "English common law does not know a general right of privacy and Parliament has been reluctant to enact one."[163] Any notion of privacy in the common law was closely tied to property rights.[164] As such, the common law of privacy remains relatively undeveloped.[165] However, there have been some changes, and there is a growing recognition of a common law right of privacy in Canada.[166] This may be due in part to the Charter jurisprudence discussed above.[167] Despite such progress, most commentators agree that a common law remedy would suffer from the same defects as the existing statutory torts.[168]

VI. Jurisdictional Disputes

When dealing with issues of electronic employee monitoring, another preliminary matter to consider is the proper forum for resolving such disputes. While the complaint-driven regimes created by the private sector privacy statutes are accessible and inexpensive, they may not offer the optimal remedy. In fact, the federal Privacy Commissioner's enforcement powers are fairly limited, such that the Office generally plays more of a mediating, ombudsman-type role.[169]

---

[163] *R. v. Brown*, [1996] A.C. 543 (H.L.) at 557. See also *Kaye v. Robertson*, [1991] FSR 62 (C.A.) at 66, Glidewell L.J.
[164] Eltis, *supra* note 31 at 488. See also *R. v. Tessling*, *supra* note 15 at para. 16.
[165] England, *Individual Employment Law*, *supra* note 68 at 139. See also England & Wood, *supra* note 73 at §8.271.
[166] Morgan, *supra* note 2 at 884. Similar changes are also underway in England: see e.g. *Douglas v. Hello! Ltd*., [2007] UKHL 21 and *Murray v Big Pictures (UK) Ltd.*, [2008] EWCA Civ 446.
[167] Morgan, *ibid.* at 898.
[168] See e.g. Levin, "Brother", *supra* note 28 at 207 and deBeer, *supra* note 3 at 403.
[169] The Commissioner's enforcement powers are set out in Part 1, Division 2 of PIPEDA. It is notable that s. 13(2) permits the Commissioner to refrain from preparing a report where "(a) the

Conversely, the British Columbia and Alberta Commissioners have been given order-making powers.[170] Thus, if an aggrieved employee wishes to raise questions about an employer's privacy practices, filing a complaint under these regimes may be their best and certainly most cost-effective option. Being an administrative process, it is easier to navigate without legal counsel and it is generally quicker than going to court.[171]

However, electronic employee monitoring issues often arise in the context of ongoing termination-related litigation. These lawsuits generally take one of two forms: employee-initiated wrongful dismissal suits or employer-initiated claims for injunctions related to misuse of confidential information or unfair competition by a former employee. Any electronic monitoring issues raised generally relate to the exclusion of evidence.[172] Of course, as noted above, it is also possible for employees to bring stand-alone privacy actions, either at common law or pursuant to a statutory regime, but the cost is usually prohibitive.

Parties may also seek to leverage a judgment or order from one of these forums in another, or rely on these jurisdictional issues to delay or prevent

---

complainant ought first to exhaust grievance or review procedures otherwise reasonably available;" or "(b) the complaint could more appropriately be dealt with, initially or completely, by means of a procedure provided for under the laws of Canada, other than this Part, or the laws of a province".

[170] AB PIPA, Part 5 (particularly s. 52(6)) and BC PIPA, Part 11.

[171] There may also be situations where privacy complaints potentially overlap with human rights complaints. Such cases would likely be determined with reference to the decision of the Supreme Court in *Regina Police Assn. Inc. v. Regina (City) Board of Police Commissioners*, [2000] 1 S.C.R. 360, where the Court set out the test for adjudicating jurisdictional disputes between two tribunals.

[172] Morgan, *supra* note 2 at 898.

proceedings in an unfavourable forum.[173] Two recent examples from the jurisprudence help to illustrate this point.

In the case of *Kellogg Brown and Root Canada v. Alberta (Information and Privacy Commissioner)*, an employee filed human rights and privacy complaints regarding the employer's pre-employment random drug and alcohol testing policy.[174] The Information and Privacy Commissioner failed to meet a time limit set out in the AB PIPA, so the employer brought a court action to determine whether the Commissioner had lost jurisdiction. After examining the situation, including other alternative remedies available to the complainant, the court concluded that the Commissioner had lost jurisdiction.

In *Osiris Inc. v. 1444707 Ontario Ltd.*, the parties were embroiled in complex litigation arising out of a franchise arrangement.[175] Certain documents relating to the dispute had been obtained by a computer hacker, so one of the parties was seeking to have them excluded, relying on arguments based on PIPEDA. The court rejected those arguments, finding that PIPEDA was to be enforced by complaints to the privacy commissioner's office. This case illustrates the limited usefulness of PIPEDA in civil litigation matters.[176]

One potential course for consolidating the current maze of competing jurisdictions with respect to electronic employee monitoring would be the creation of a single "labour court", responsible for handling all employment-related

[173] Levin, "Brother", *supra* note 28 at 209-210.
[174] 2007 ABQB 499.
[175] [2005] O.T.C. 1101 (S.C.J.).
[176] See also *Ferenczy v. MCI Medical Clinics* (2004), 70 O.R. (3d) 277 (S.C.J.).

complaints.[177] If employee privacy protections were eventually built into provincial employment standards legislation, a 'one-stop shop' for the informal and expeditious resolution of workplace disputes, including matters involving electronic monitoring, would certainly be an improvement on the current situation.

VII. International Context

While a thorough review of international workplace privacy laws is beyond the scope of this thesis, it is important to situate Canadian laws in their international context. As Lawson and Jeffery note, privacy is recognized as an aspect of human dignity in three important international human rights documents, namely, article 12 of the *Universal Declaration of Human Rights*, article 8 of the *European Convention for the Protection of Human Rights and Fundamental Freedoms* and article 17 of the *International Covenant on Civil and Political Rights*.[178]

These pronouncements are reflective of the European approach to privacy, which is to treat it as a fundamental human right.[179] This, in turn, is tied to the civil law's conception of privacy and the right to private life. For this reason, the law in Quebec has developed, and has the potential to keep developing, in line with the more privacy-friendly European approach.[180]

The American development of privacy law has been much more focused on property rights and managing the reasonable expectations of employees than

---

[177] England, *Individual Employment Law*, *supra* note 68 at 218. A similar proposal has been considered by the Ontario government: Ministry of Labour, *Looking Forward: A New Tribunal for Ontario's Workplaces* (Consultation Paper), February 2001, online: Ontario Ministry of Labour <http://www.ontla.on.ca/library/repository/mon/1000/10293245.pdf>.

[178] Lawson, *supra* note 7 at 64. See also Morgan, *supra* note 2 at 872 and Radwanski, *supra* note 10 at 2.

[179] For an introduction to the European approach, see Eltis, *supra* note 31.

[180] Levin, "Brother", *supra* note 28 at 220. See also Eltis, *ibid.* at 480.

on European notions of human rights, autonomy and dignity.[181] Some critics complain that the notions of privacy and liberty have been conflated in the American jurisprudence, particularly in cases decided under the Fourth Amendment of their Constitution.[182] As Eltis explains, in the United States, employees must prove their privacy rights whereas, in France, employers must justify any surveillance they undertake.[183]

According to Levin, the Canadian approach occupies the middle ground between the American property-based approach and the European dignity-based approach; "[i]nstead, it appears to be a unique Canadian approach, based on the value of trust."[184] Levin posits that Canadian employers recognize that undue intrusions into employees' privacy have a negative effect on productivity and morale; such measures make employees feel that they are being spied upon because they are untrustworthy. Conversely, respect for employees' privacy can foster positive attitudes and greater efficiency, as employees respond to the trust their employers have demonstrated. However, he goes on to remark that:

> Luckily for *employers*, the courts in the common-law jurisdictions of Canada have yet to adopt, fully or partially, an approach to workplace surveillance based on the dignity of the monitored workers, although the jurisprudence is already well developed in Quebec for such an approach. The examination of whether workplace surveillance for productivity measurement purposes is permissible under current legislation and case law must take therefore another perspective into account, and ask whether such surveillance is [p. 221] reasonable. ... Care must be taken here to focus on the employer's conduct, but unfortunately many Canadian

[181] An introduction to the American law on this subject may be found in Morgan, *supra* note 2 at 865; Eltis, *ibid.*; Levin, "Brother", *ibid.* at 221. For a fuller review, see Uteck, *supra* note 4 at 102-130.
[182] See e.g. Uteck, *ibid.* at 83.
[183] Eltis, *supra* note 31 at 483.
[184] *Under the Radar*, *supra* note 14 at 15.

> employers follow the US lead, and focus on the worker's expectations.[185]

It remains to be seen whether Canadian law will be drawn to either one of these extremes or whether it will continue to forge a new path through the middle ground. While economic conditions may result in limited or stunted privacy protections, the growing pervasiveness of human rights and the resulting rights-based discourse bode well for increased employee privacy protections in Canada in the future.

VIII. Relevant Jurisprudence

A. Possible Analytical Approaches

An initial analytical difficulty in approaching electronic employee monitoring cases is determining the appropriate taxonomy. A number of possible approaches present themselves, namely: sectoral; locational; temporal; method of monitoring; decision-maker/issue involved; outcome; or type of technology. Each of these approaches will be considered in turn.

1. Sectoral

As noted above, different privacy regimes apply to the public and private sectors. The fact that a different legal framework is involved may help to explain disparate outcomes in similar cases in these two sectors. In particular, the applicability of the Charter may result in greater privacy protections being accorded to public sector workers.

[185] Levin, “Brother”, *supra* note 28 at 220-221 [emphasis in original].

2. Locational

Another possible approach to categorizing electronic monitoring cases is to focus on the location of the surveillance, either at the workplace or off-site.[186] As Veilleux explains, "une personne salariée qui n'est pas au travail a une attente raisonnable élevée au respect de sa vie privée puisqu'elle n'est plus soumise au contrôle de l'employeur."[187]

3. Temporal

There are two aspects to a potential temporal division of electronic monitoring cases. First, the length of time over which monitoring occurs may be a factor to consider.[188] Second, whether the monitoring occurs while the employee is on- or off-duty may also affect the result. In this way, a temporal classification approach is similar to a locational approach, in that when most workers are off-site they are also off-duty. Combining these two approaches may improve the accuracy of their results.[189]

---

[186] See e.g. *Sherrard*, *supra* note 35 at 290.

[187] Veilleux, *supra* note 13 at 22. It is notable that this is not generally the case with respect to video surveillance. As Lorne A. Richmond states in "Employee Use of E-mail and the Internet: A Union Perspective" (2001-2002) 2 Lab. Arb. Y.B. 45 at 46, in the context of video surveillance: "Generally speaking, off-site surveillance is permissible in certain circumstances, and evidence derived from such surveillance has more or less routinely been admitted to demonstrate benefit fraud. Surveillance in the workplace at large, on the other hand, is rarely tolerated. An exception to the general rule is surveillance that targets individual employees on the basis of a reasonable suspicion of misconduct." While this is true of video surveillance, as in the workplace visible evidence could be captured by fellow employees simply viewing the incident, the same is not necessarily true of e-mail and the internet misuse, where both on- and off-site misuse is relatively 'invisible'.

[188] See e.g. C.L. Rigg, "The Right to Privacy in Employment: An Arbitrator's Viewpoint" (1991) 1 Lab. Arb. Y.B. 83 [Rigg] at 88.

[189] This combined approach would offer four categories for classification: (1) on-duty, on-site; (2) off-duty, on-site; (3) off-site, on-duty; and (4) off-site, off-duty. It might be posited that surveillance is more permissible in the first category of cases, and least permissible in the latter category. However, in comparing the third and fourth categories, surveillance would likely be more acceptable in the third situation.

4. Classification Based on Method of Monitoring (including Overt versus Covert)

This particular method of classification has a number of aspects.[190] First, the method of monitoring may be categorized based on the nature of the privacy interest at stake. Second, categorization may be based on the extent of the invasion of that privacy interest. Third, and perhaps most obvious, the manner in which the monitoring takes place may be taken into account. This consideration may include whether the monitoring was overt or covert and random or targeted.

As a general rule, covert surveillance is less acceptable than overt surveillance.[191] As well, it is generally preferable if surveillance is undertaken only after a reasonable suspicion has formed regarding a particular employee, rather than on a random, indiscriminate or universal basis.

5. Classification Based on the Decision-Maker or Issue Involved

As described above, there are several forums for the resolution of workplace privacy disputes, including privacy commissioners and the courts. Furthermore, different approaches may be taken by decision-makers in different provinces. Understanding these distinctions may assist with classifying the cases and reconciling their outcomes. It may be particularly important to bear in mind the extent of each decision maker's remedial jurisdiction.

6. Classification Based on Outcome or Impact on the Employee

This pragmatic approach would classify cases based on the outcome for the parties involved. For instance, one could assess how a particular electronic

[190] A thorough review of this approach is undertaken by Rigg, *supra* note 188, especially at 87-89.
[191] See e.g. deBeer, *supra* note 3 at 386.

monitoring technology is treated in the context of wrongful dismissal claims, as opposed to solely evidentiary matters or other disputes not involving the termination of the employment relationship. It may be that if an employer's violation of an employee's privacy affected the employee's livelihood (*i.e.*, resulted in termination), the violation will meet with less acceptance in the courts. Alternatively, cases may be catalogued based on the nature of the remedy granted.

7. Classification Based on the Type of Technology Involved

Another potential approach to the developing case law regarding electronic employee monitoring would divide the cases based on the type of technology at issue therein. This is the approach that will be adopted here, along with a consideration of the other factors mentioned above. In this way, it may be possible to determine whether the nature of the technology affects the outcome of the case, and whether certain electronic monitoring technologies are more readily accepted than others.[192]

B. Review and Analysis of Relevant Jurisprudence

1. Computer, Internet and E-mail Cases

(a) Reasonable Expectations versus Objective Reasonableness

The 'reasonable expectations versus objective reasonableness' debate outlined above looms large in the context of monitoring employees' computer, internet and e-mail use. Much of the initial academic commentary and case law, building upon the American experience, focused on employees' reasonable

[192] However, the adoption of this approach should not be construed as a rejection of an overarching, technology-neutral approach to electronic employee monitoring.

expectations, which in turn was influenced by the question of ownership.[193] On this model, it was concluded that employees had "little or no expectation of privacy within the workplace", so covert or overt electronic surveillance was permissible.[194] Where the employer owned the computer or provided the internet or e-mail access, employees' reasonable expectations of privacy were automatically lowered.[195] As Poirier observes:

> The work environment presents circumstances that can have an impact on employees' legitimate expectations of privacy in their e-mail usage. First, the employer generally owns the e-mail system. Second, the information contained in e-mail messages at work is likely to be business-related and thus less deserving of privacy protection. Third, the very nature of the employment relationship allows the employer to maintain a certain level of control over the workplace in order to protect its legitimate business interests. Finally, it is possible that certain policies and representations have been made by the employer concerning the permitted use and possible surveillance of the e-mail system, directly affecting employees' expectations of privacy.[196]

However, a number of commentators objected to the resolution of such issues solely on the basis of ownership of the technology.[197] A popular analogy was to company pens: if a personal letter was written with a company pen, did that give the employer a right to read it?[198] It was also noted that using someone else's telephone did not give them the right to eavesdrop on the conversation.[199]

---

[193] As discussed in Levin, "Brother", *supra* note 28 at 222.
[194] Geist, *supra* note 5 at 162. See also Klein, *supra* note 38 at 56-57; McIsaac, *supra* note 16 at 2.5.4.3(b); Rasky, *supra* note 20 at 221.
[195] Anderson, *supra* note 21 at 679. See also Poirier, *supra* note 19 at 100 and Rasky, *supra* note 20 at 223.
[196] Poirier, *ibid.* at 95.
[197] See e.g. Poirier, *ibid.*; Veilleux, *supra* note 13 at 27. See also Eltis, *supra* note 31 at 501, where the author urges tribunals in Quebec to reject the American approach to workplace privacy.
[198] Morgan, *supra* note 2 at 890, n. 177.
[199] Poirier, *supra* note 19 at 97. However, this analogy has limited relevance in the employment context, where the employer both owns the technology and is paying the employee to use it for business, not personal, purposes.

Poirier further argues that the fact that e-mail may be intercepted does not negate a reasonable expectation of privacy regarding its contents.[200] By way of illustration, this is akin to saying that since burglars have developed effective tools for gaining entry to houses, homeowners should expect to be robbed. If limits on privacy rights are left to be defined by technology, there will soon be very little – if anything – left to protect.[201] As Sherrard aptly observes, "[t]he question is no longer whether employers can monitor electronic communication, but whether they should."[202]

As noted above, the focus has now shifted to the objective reasonableness of electronic employee monitoring. Klein proposes the following factors for assessing the propriety of such monitoring:

- Nature of the monitoring;
- Employee's awareness of the monitoring;
- Whether the monitored activity is classified as "business" or "private"; and
- The egregiousness of the monitoring.[203]

Similarly, Geist has proposed six factors to consider in assessing the reasonableness of such surveillance:

---

[200] Poirier, *ibid.* at 92 and 94.

[201] David Mason *et al.* comment on this "essentially determinist position" in "Getting Real about Surveillance and Privacy at Work" in Steve Woolgar, ed., *Virtual Society? Technology, Cyberbole, Reality* (Oxford: Oxford University Press, 2002) 137 [Mason] at 139. See also Radwanski, *supra* note 10 at 6, 7 and 9: "In other words, as I have often said, our privacy has been protected by default. And that default point slips away as technology advances...[p. 7] The default protection is gone now. Technological limits won't preserve the core of privacy much longer…[p. 9] Technology is not going to limit our ability to invade privacy any more. We have to impose our own limits." In response, some commentators argue that, in the future, privacy will be protected because technology places too much information at our disposal and we will suffer information overload: see e.g. Evan VanDyk, "Memory" *Slaw* (16 October 2007), online: Slaw <http://www.slaw.ca/2007/10/16/memory/>.

[202] Sherrard, *supra* note 35 at 294.

[203] Klein, *supra* note 38 at 57. See also McIsaac, *supra* note 16 at 2.5.4.3(b).

- The target of the surveillance;
- The purpose of the surveillance;
- The prior use of alternatives to surveillance;
- The surveillance technology;
- The adequacy of the notice provided to the target of the surveillance; and
- The implementation of the surveillance.[204]

Recognizing the need for proper employee notification regarding such surveillance, all commentators agree that employers should have policies in place which outline when and how electronic employee monitoring may occur.[205] Conversely, the failure to enact a policy limiting employees' personal use of computers, internet and e-mail may be interpreted as implied consent to such use.[206] The ubiquity of internet access and e-mail communications is giving rise to a growing recognition that a total ban on the personal use of such facilities by employees during working hours is unrealistic.[207] Just as the occasional personal telephone call is now common in the workplace, it is foreseeable that a limited amount of personal computer, internet and e-mail use will become the accepted workplace norm.

---

[204] Geist, *supra* note 5 at 155. See also 178 and 187. It is questionable whether privacy-sensitive treatment of data obtained through electronic employee monitoring could save an otherwise dubious scheme, but it may assist in casting the entire process in a more privacy-friendly light.
[205] See e.g. Anderson, *supra* note 21 at 679; Morgan, *supra* note 2 at 902; Brunette, *supra* note 83 at 71; Poirier, *supra* note 19 at 102-104; Rasky, *supra* note 20 at 228; Sherrard, *supra* note 35 at 299; Jason Young, "The Blogger in the Workplace: Considerations for Employers and Employees" (2005) 6 Internet & E-Commerce Law in Canada 9 [Young] at 11; Lifshitz, "Blogging", *supra* note 25 at 96; Lauzon, *supra* note 13 at 53. At 187, *supra* note 5, Geist suggests that "...policies must be respectful of privacy norms and seek to achieve an appropriate balance between surveillance needs and privacy interests." An interesting problem is posed by the monitoring of incoming e-mail messages, as it is unlikely that the sender could provide advance consent to such monitoring: Poirier, *supra* note 19 at 103.
[206] Poirier, *ibid.* at 101.
[207] Eltis, *supra* note 31 at 501, n. 125.

Of course, computer usage policies are not enacted simply to lower employees' reasonable expectations of privacy; with the advent of laws such as PIPEDA and its provincial counterparts, the provisions of the policy itself must also be objectively reasonable. It will be easier to meet this test if any monitoring undertaken is targeted and based on a reasonable suspicion.[208] Except in very exceptional circumstances, it would be difficult to characterize wholesale, indiscriminate monitoring of employees' computer, internet and e-mail use as objectively reasonable.[209]

Nevertheless, it should be remembered that there are limits on the privacy rights that may be asserted by employees. Generally speaking, informational privacy rights only extend to information that can be linked to an identifiable individual. Thus, monitoring the size of computer files downloaded over the corporate network would not necessarily violate employees' privacy.[210] Veilleux posits that compiling a list of websites visited by employees would not infringe their privacy rights.[211] Poirier admits that e-mail headers, which reveal the identity

---

[208] Durnford, *supra* note 24 at 68.
[209] Poirier, *supra* note 19 at 104. See also Veilleux, *supra* note 13 at 44-45.
[210] Morgan, *supra* note 2 at 901.
[211] Veilleux, *supra* note 13 at 27. An analogy might also be drawn to *Telecommunications Company Does Not Improperly Collect or Use Employee Statistics* (14 April 2003), PIPEDA Case Summary #153, online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030414_3_e.asp>, which dealt with the collection of operators' call statistics by a telecommunication company. But see the more recent *Condition of Washrooms Prompts Management to Monitor Facilities* (4 April 2007), PIPEDA Case Summary #379, online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/cf-dc/2007/379_20070404_e.asp>. In that case, there were concerns about the state of the workplace washroom. The company monitored who used the washroom by means of visually monitoring who entered the washroom. This was done by employees watching the washroom door and making a list of who entered, not by using a video camera or other electronic means. It might be argued that placing a video camera in the washroom would have been equivalent to indiscriminately monitoring all employees' computer, internet and e-mail usage. Conversely, making a list of the websites visited by employees could be analogized to the facts of this case, which held that even such forms of surveillance could be considered privacy-invasive.

of the sender and the recipient of the message, may not be protected by employee privacy rights.[212]

Furthermore, there are a number of alternative methods for accomplishing the objectives of electronic employee monitoring. Durnford counsels that:

> ...[E]mployers should consider less invasive measures such as blocking certain sites, warning employees about prohibited behaviour and the consequences, and purging their systems regularly so as to discourage employees from storing personal files on the company computer.[213]

Employees could also be encouraged to mark e-mails as either "business" or "personal", to assist in rendering the employer's electronic monitoring regime less invasive and more privacy-friendly.[214]

In light of perceived threats to their privacy, employees may also look for privacy-enhancing alternatives. By seeking out internet-based e-mail services, instead of relying on the e-mail system provided by the employer, they may signal that they expect greater privacy in such communications. This has the added benefit of reducing the employer's reputational risks, as such web-based e-mail addresses are usually not associated with the company. Employees may

---

[212] Poirier, *supra* note 19 at 98.

[213] Durnford, *supra* note 24 at 68. A recent American case highlights the need for vigilance on the part of employers in this respect. Michael Fiola was fired as a worker's compensation fraud investigator after information technology ("IT") administrators found cached images of child pornography in the temporary internet files of his web browser. However, Fiola hired forensic experts to prove that the pornography was due to malware on his laptop. "His laptop initially attracted attention because its wireless usage was four times higher than that of his co-workers. But because the IT department hadn't properly configured the agency laptop and antivirus software wasn't working on the machine, it was riddled with Trojans and viruses, in addition to the malicious software that was bringing up the porn sites": Elinor Mills, "State worker cleared on child porn charges that were due to malware" *CNET* (17 June 2008), online: CNET <http://news.cnet.com/8301-10784_3-9970660-7.html>.

[214] Poirier, *supra* note 19 at 97-98. This approach is advocated by the United Kingdom's Information Commissioner's Office (see "The Employment Practices Code", §3.2.8 <online: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/employment_practices_code.pdf>).

also look to encryption technologies to protect their personal files and messages on company computers and networks. While this may provide a greater measure of privacy protection, the mere usage of advanced encryption technology may kindle an employer's suspicions and prompt an employer to engage in further, more invasive monitoring.

(b) Consequences of Employees' Electronic Misconduct

While the law regarding electronic employee monitoring remains unsettled, the fundamental pragmatic concern for employers is determining what they can do when they discover that an employee is misusing corporate computer, internet or e-mail resources. Based on the existing case law, employers may be surprised to find that only rarely will such misconduct constitute stand-alone cause for summary dismissal.[215] As Ball explains, "[w]hile excessive personal e-mail may constitute a work performance issue, poor performance will justify cause for summary dismissal in relatively few circumstances."[216] In assessing the propriety of any discipline imposed for this type of 'electronic misconduct', a number of factors will be reviewed, including:

- Any policies in place at the time of the alleged misconduct;
- Whether the employer condoned the alleged misconduct or allowed a permissive culture to develop with regard to the impugned activity; and

---

[215] See e.g. *Milsom v. Corporate Computers Inc*. (2003), 27 C.C.E.L. (3d) 26 (Alta. Q.B.) [*Milsom*]; *Di Vito and Mathers v. Macdonald Dettwiler & Associates Ltd.* (1996), 21 C.C.E.L. (2d) 137 (B.C.S.C.) [*Di Vito*]; *Boisvert c. Industrie Machinex Inc.*, D.T.E. 2002T-185 (Que. C.T.) [*Boisvert*]; *Koo Employment Insurance Claim Appeal* (10 September 1998), CUB 42710, online: EI <http://www.ei-ae.gc.ca/policy/appeals/CUBs/40000-50000/42000-42999/42710e.html>; *Gilles c. Ciba Spécialités chimiques Canada inc.*, 2008 QCCRT 134 [*Gilles*]; *Plotogea v. Heartland Appliances Inc*. (2007), 60 C.C.E.L. (3d) 216 (Ont. S.C.J.) [*Plotogea*].

[216] Ball, *supra* note 81 at 11:195. See also Brunette, *supra* note 83 at 69.

- The nature of the material and the misconduct engaged in by the employee.[217]

A review of the existing jurisprudence reveals that most of the reported cases regarding employee misuse of computers, internet and e-mail involve the viewing, downloading, sending or receiving of sexually explicit material.[218] As Ball notes, "...when the pornography involves something which is criminally forbidden, it may very well be that progressive discipline would not be required by the court."[219] It seems likely that many employees may misuse computers, internet and e-mail in other ways (such as playing games, conducting personal business, visiting websites and exchanging e-mails unrelated to workplace matters). However, such cases rarely result in court proceedings. Thus, it would seem that an employer's response is often motivated by the type of content at issue; if an employee is reading too much news or checking the sports scores too often, the employer likely cautions the employee, perhaps monitors them in the future, and the matter is laid to rest. However, where the content is more objectionable, harsher measures are imposed, up to and including summary dismissal. It would therefore seem that electronic misconduct involving non-objectionable content is

[217] Brunette, *ibid.* at 70.
[218] It is interesting to note that while "pornography" is neither a term of art nor a legal term with an accepted definition (though "child pornography" is defined in s. 163.1(1) of the *Criminal Code*), it is the term usually employed in these types of cases. It does not appear that there is any significance in this choice of terminology, though further analysis of the application of concepts of "obscenity", "pornography" and "sexually explicit materials" in such cases may yield further insight into this matter. In this thesis, the phrase "sexually explicit material" will be used to encompass all of these concepts, though the term "pornography" is used when it is contained in a quote.
[219] Ball, *supra* note 81 at 11:195.

more acceptable than misconduct involving sexually explicit materials.[220] As Levin observes:

> The reality is that in practice most employers turn a blind eye to private use of workplace resources. As long as employees operate under the radar with reasonable use, they will not be challenged on their personal use of employer resources.[221]

This trend may be tied to the increasing acceptance of limited personal use of computers, internet and e-mail in the workplace described above.

(c) Modes of Electronic Employee Monitoring Utilized in Canada

Only a few reported electronic misconduct cases have stemmed from routine electronic employee monitoring.[222] Instead, such misconduct is usually discovered inadvertently or brought to light after an employee is terminated. The existing case law may be divided into five categories, namely:

- Cases where an unintended party is exposed to the misconduct;
- Cases where the misconduct is reported by co-workers;
- Cases where information about employees' electronic misconduct is uncovered during the course of a different type of investigation;

---

[220] One case that defies categorization is that of *Québec (Commission des normes du travail) c. Bourse de Montréal inc.*, [2002] R.J.Q. 807 (C.S.). There, an IT employee was dismissed because he (1) stored a copy of a computer virus to examine it further (instead of destroying it immediately); (2) ran the SETI@home program on company machines while they were idle; and (3) visited a "hackers" website and downloaded a program for cracking passwords. The SETI@home program was developed by the University of California, Berkeley. As described on its website (http://setiathome.berkeley.edu/), "SETI@home is a scientific experiment that uses Internet-connected computers in the Search for Extraterrestrial Intelligence (SETI). You can participate by running a free program that downloads and analyzes radio telescope data." As described in para. 6 of the decision, "...chaque usager de ce site prête en quelque sorte les services de son ordinateur pour analyser et décrypter les signes pouvant provenir de l'espace. Les ordinateurs ne sont utilisés que lorsqu'il n'y a pas d'autres tâches à accomplir." No damage was proven by the employer and the employee was contrite. In the end, the court sided with the employee.

[221] *Under the Radar*, *supra* note 14 at 17.

[222] It may be that cases involving continuous monitoring are never brought to trial because employees (or their counsel) view them as 'unwinnable'. Alternatively, wholesale proactive monitoring may in fact deter electronic misconduct, and thus such workplaces do not give rise to these types of cases.

- Cases involving *ex post facto* computer forensics; and
- Cases involving proactive monitoring.

In the first category, involving the exposure of unintended parties to the misconduct, employees engaged in misconduct may inadvertently send an e-mail to an unintended recipient.[223] As well, non-work-related images on a computer screen may be viewed by an employee's supervisor or co-worker as they pass the employee's work station.[224]

Employees who were intentionally exposed to electronic misconduct in the hopes that they might participate in it may not necessarily appreciate receiving inappropriate content; they may decide to bring it to management's attention.[225]

The third category of cases usually involves sexual harassment investigations.[226] The alleged harassment may not necessarily arise out of computer-related activities, but the alleged harasser's computer may be scanned as part of the investigation, in any event. Other investigations might also uncover evidence of employees' electronic misconduct, such as those relating to workplace accidents or human rights violations.[227] For instance, in *Soplet v. Bank of Nova Scotia*, an investigation into the sale of drugs in the workplace led to finding inappropriate files on an employee's computer.[228]

---

[223] See e.g. *Dhoot v. First Calgary Savings & Credit Union*, 1998 CarswellAlta 1291 (Q.B.).
[224] See e.g. *Boisvert*, *supra* note 215.
[225] See e.g. *EPCOR Utilities Inc.* (10 April 2007), Investigation Report #P2007-IR-004, online: Alberta Information and Privacy Commissioner <http://www.oipc.ab.ca/ims/client/upload/Investigation%20Report%20P2007_IR_004.pdf> and *Di Vito*, *supra* note 215.
[226] See e.g. *Foerderer*, *supra* note 79 and *Seaton v. Autocars North (1983) Inc. (c.o.b. North Toronto Mazda)*, [2000] O.T.C. 348 (S.C.J.) [*Seaton*].
[227] The doctrine of after-acquired cause (*supra* note 79) may be relevant in such cases.
[228] (2007), 57 C.C.E.L. (3d) 269 (Marvy) [*Soplet*].

The most common method of bringing employees' electronic misconduct to light is a post-termination review of their computer-based activities.[229] This type of forensic review may be done by the employer or may involve a third party hired by the employer.[230] This type of forensic review does not necessarily have to take place post-termination. Some other event may cause an employer to look more closely at an employee's computer, internet or e-mail usage. For instance, in *Blais c. Société des Loteries Vidéos du Québec Inc.*, one of the employee's e-mails was blocked by the company's firewall.[231] In *Bell v. Computer Science Corp.,* a keystroke logging device was discovered on an employee's computer, which prompted a thorough inspection by the employer's IT department.[232] In *Gilles*, the employee's habit of storing photographic images and videos on his computer was discovered after his computer stopped working and had to be repaired by the company's IT staff.[233]

To date, there are only a few examples in the case law involving proactive, systematic electronic employee monitoring. In *Parkland Regional Library*, the employer attempted to capture data about an employee's computer activities by

---

[229] See e.g. *Manchulenko*, *supra* note 79; *Milsom*, *supra* note 215; *Harris Scientific Products Ltd. v. Araujo*, 2005 ABQB 603 [*Harris*]; *Atwood v. CAC Computers & Communications Inc.*, 2001 BCSC 875 [*Atwood*]; *Potvin c. Malartic (Ville)*, 2003 CarswellQue 2093 (C.S.) [*Potvin*].

[230] For instance, in *Gilles*, *supra* note 215, an outside firm was hired to reconstruct the employee's hard drive and deleted files. In *Harris*, *ibid.*, logs of an employee's account activity were obtained from the employer's internet service provider. In *Re Langley Cruiseshipcenters Ltd.* (14 December 2006), Order P06-05, online: British Columbia Information and Privacy Commissioner <http://www.oipc.bc.ca/PIPAOrders/2006/OrderP06-05.pdf> [*Langley*], an investigator was hired to review employees' e-mails. Similarly, in *Potvin*, *ibid.* a specialist was hired to analyze Potvin's computer after his termination.

[231] 2003 QCCRT 14 [*Blais*].

[232] 2006 CarswellOnt 9143 (S.C.J.), aff'd 2007 ONCA 466, leave to appeal refused, [2007] S.C.C.A. No. 393 (QL) [*Bell*].

[233] *Supra* note 215.

installing keystroke logging software.[234] In that case, the Alberta Information and Privacy Commissioner found that it was a breach of the governing privacy legislation for the employer to surreptitiously install such software on the employee's computer.[235] In *Bongeli v. Citibank Canada*, a customer service representative doing work for Citibank was implicated in a fraud scheme.[236] His questionable transactions were identified by fraud prevention software, and proof regarding his activities was obtained by analyzing logs of his past computer activities. While there are not many details provided, in *Plotogea*, sexually explicit materials were discovered on the employee's computer in a "routine check".[237] Subsequent monitoring confirmed that the employee was still accessing such materials.

(d) Special Issues Related to Employees' Use of Computers, Internet and E-mail

(i) Disclosure of Confidential Information

As noted above, one of the reasons employers monitor their employees' electronic activities is to prevent the disclosure of confidential corporate information, particularly to their competitors. An early illustration of this phenomenon may be taken from the widely-reported case involving two companies, Borland and Symantec. It was alleged that Eugene Wang, a former

---

[234] (24 June 2005), Order F2005-003, online: Alberta Information and Privacy Commissioner <http://www.oipc.ab.ca/ims/client/upload/F2005-003.pdf>.

[235] See also *University of British Columbia* (24 September 2007), Order F07-18, online: British Columbia Information and Privacy Commissioner <www.oipc.bc.ca/orders/2007/OrderF07-18.pdf>. The University has applied for judicial review of the Adjudicator's order: James Kosa, "Canadian University Challenges Order Regarding Employee Monitoring" *E-Tips* (7 November 2007), online: Deeth Williams Wall <http://www.dww.com/?p=1175#more-1175>.

[236] [2004] O.T.C. 686 (S.C.J.), aff'd [2006] O.J. No. 263 (C.A.) (QL).

[237] *Supra* note 215.

Borland executive, had used the Borland e-mail system to disclose confidential corporate information to its competitor, Symantec, shortly before he left Borland to take a position with Symantec.[238] Similar concerns prompted the employer to hire an investigator to review employees' e-mail correspondence in the *Langley* case.[239] In *Nesbitt Burns Inc. v. Lange*, the employer sought an injunction against a former employee, alleging that he was using the employer's e-mail system to solicit clients.[240] Similarly, allegations of improper post-termination remote internet and e-mail access formed part of the basis for an *Anton Piller* order in the *Harris* case.[241]

(ii) Lack of Progressive Discipline/Notification or Condonation

Failing to notify an employee about an employer's expectations regarding computer, internet or e-mail use, or failing to vigorously enforce existing policies often stymies attempts by employers to summarily dismiss employees for electronic misconduct.[242] For instance, in *Re Avante Furniture Manufacturing (1992) Ltd.*, the employee was not warned that misusing computer privileges could result in termination.[243] In *Dhoot*, the employer overreacted when an employee sent an e-mail to co-workers saying how much work she could get done while her boss was away from the office.[244] Such conduct was only

---

[238] Poirier, *supra* note 19 at 100, n. 89. The litigation was later settled: "Borland, Symantec call truce" *CNET* (14 February 1997), online: CNET <http://news.cnet.com/Borland,-Symantec-call-truce/2100-1023_3-271125.html>.
[239] *Supra* note 230. The British Columbia Information and Privacy Commissioner found that such an investigation was authorized by BC's PIPA in the circumstances.
[240] (2000), 16 C.C.E.L. (3d) 317 (Ont. S.C.J.). The injunction was not granted.
[241] *Supra* note 229. However, as this was a misrepresentation, damages were awarded to the employee.
[242] Lauzon, *supra* note 13 at 52.
[243] [2001] B.C.E.S.T.D. No. 64 (QL) [*Avante*].
[244] *Supra* note 223.

deserving of a reprimand or warning. In the result, the employee was awarded damages for constructive dismissal. Similarly, in *Manchulenko*, *ex post facto* evidence of the employee's misuse of his employer-provided e-mail account was insufficient support for the employer's decision to terminate his employment without notice.[245] Again, it was held that the employee should have been warned or reprimanded about such conduct, in order for the employer to rely upon it in the wrongful dismissal action. In *Services d'administration P.C.R. ltée c. Daigle*, the employer was found to lack just cause for dismissal.[246] Instead of having a computer usage policy in place, it condoned the employee's activities.[247] An employer may also be unable to rely on evidence of an employee's electronic misconduct if it is aware of such evidence but does not allude to it in the termination letter.[248] To hearten employers, it should be mentioned that there are a few examples from the case law where employees were found to have been aware of the rules regarding computer usage; their terminations were justified.[249]

(iii) Sexual Harassment and Sexually Explicit Materials

Most of the cases regarding electronic monitoring of employees' computer, internet and e-mail usage involve sexually explicit materials.[250] What must be

---

[245] *Supra* note 79.
[246] [2003] J.Q. no 121 (C.S.), aff'd [2003] J.Q. no 4562 (C.A.) [*Daigle*].
[247] See also *Gilles*, *supra* note 215.
[248] See e.g. *Soplet*, *supra* note 228.
[249] See *Bhamre Employment Insurance Claim Appeal* (17 March 1997), CUB 42012A, online: EI <http://www.ei-ae.gc.ca/policy/appeals/cubs/40000-50000/42000-42999/42012AE.html> and *Blais*, *supra* note 231. However, it should be noted that in *Blais*, the employee's improper e-mail and internet use would only have warranted a suspension, despite the fact that he had been previously warned and that the employer's policy was clear and well-known. His termination was upheld because this misconduct was combined with theft.
[250] See e.g. *Foerderer*, *supra* note 79; *Tremblay*, *supra* note 30; *Gilles, supra* note 215; *Pinto v. BMO Nesbitt Burns Inc.* (2005), 40 C.C.E.L. (3d) 293 (Ont. S.C.J.); *Plotogea, supra* note 215; *Potvin, supra* note 229; *Seaton, supra* note 226; *Soplet, supra* note 228.

understood is the link between using workplace computers, internet and e-mail to view, download, receive and distribute sexually explicit materials and sexual harassment claims by other employees. While repeated downloading or electronic distribution of sexually explicit materials in the workplace, contrary to clear policies and formal warnings (especially where the conduct could be categorized as criminal) may justify the summary dismissal of the offender, it may also give rise to sexual harassment complaints by other employees.[251] As stated earlier, this is one of the reasons why employers say electronic employee monitoring is necessary, in order to prevent sexual harassment in the workplace and, in any event, limit their liability for same.

(iv) Electronic Evidence in the Employment Context

Aside from concerns regarding sexual harassment in the workplace, another reason advanced by employers as justification for electronic employee monitoring is their need to comply with electronic discovery requests in litigation matters. A by-product of this electronic evidence collection process is the reality that such evidence may also be used against employees in post-termination proceedings.[252]

In particular, electronic evidence can be particularly effective in defending against wrongful dismissal claims. For instance, in *Atwood*, the employee sued her former employer for wrongful dismissal, claiming that she had suffered sexual

[251] See e.g. *Foerderer, Pinto* and *Seaton*, *ibid.*
[252] See e.g. *Pacific Northwest Herb Corp. v. Thompson*, 1999 CarswellBC 2738 (S.C.); *Lovelock v. DuPont Canada Inc.*, [1998] O.J. No. 4971 (Gen. Div.) (QL); *Atwood*, *supra* note 229; *Bell, supra* note 232; *Harris, supra* note 229.

harassment.[253] However, the employer was able to produce copies of her e-mails and instant messages to demonstrate that she was one of the main participants in the raunchy work environment. As a result, the claim was dismissed.

(v) Damage to Employer's Reputation

Another concern for employers arising out of their employees' computer, internet and e-mail use relates to the protection of the employer's reputation. A common example relates to the forwarding of e-mail messages. Many employers provide e-mail addresses with the company's name as part of the domain name (*e.g.*, employee@companyname.com), so any e-mail sent by an employee can be easily identified with the company. Furthermore, many employees include standard signature files in all of their e-mail messages, which place their work contact information in the body of the e-mail message. Employers are concerned that this information may be linked to inappropriate e-mail content, which would reflect poorly on them, as they may be seen as giving tacit approval to it.[254]

One such example may be drawn from the existing jurisprudence. In *Arpin c. Grenier*, an employee posted a controversial political message on a public electronic bulletin board, signing it with his company-provided e-mail address (which contained the company's name).[255] His employer later found it difficult to obtain financing.[256] While a small amount of damages were awarded to the

[253] *Atwood*, *ibid.*
[254] Or, at the very least, the rigorousness of their hiring processes may be questioned.
[255] [2004] J.Q. no 6876 (C.Q. - Petites créances) (QL).
[256] As stated in para. 7 of the case, "[l]e président de la demanderesse témoigne qu'il rencontrait certaines difficultés à obtenir du financement dernièrement. Il effectue donc une recherche afin de connaître pourquoi il recevait un accueil plus froid des investisseurs potentiels."

employer, the case is a good illustration of how employees' conduct on the internet can affect their employers' reputations.

Another, more elaborate example along the same lines may be taken from the recent case of *Inform Cycle Ltd. v. Draper*.[257] The employer's website was www.informcycle.ca. A disgruntled former employee named Draper purchased the similar domain name of www.informcycle.com. At first, he redirected traffic from the site to his new employer's website. Draper's new employer, Rebound, was one of Inform Cycle's direct competitors. After a few weeks, Draper redirected the traffic from www.informcycle.com to a "gay pornographic" website, then left the country to go on an extended holiday. One of the owners of Rebound contacted Draper while he was on holidays to get the password to cancel the forwarding of the www.informcycle.com website to the "gay pornographic" website. Draper was found liable for passing-off, defamation and "knowingly and deliberately" undertaking the registration and forwarding of the www.informcycle.com website. General damages were assessed at $10,000 and an additional $5,000 in punitive damages was awarded. This case demonstrates the necessity of vigilance on the part of employers to monitor their online presence and reputation; it also demonstrates their vulnerability to electronic attacks by disgruntled employees.[258]

[257] 2008 ABQB 369.

[258] As Lee notes, specifically with respect to blogging, *supra* note 51 at para. 9: "In response to the threat of critical, false, disparaging or confidential information being posted by anonymous anti-employer bloggers on the internet, many employers hire 'scouring agencies'...to comb internet blogs, message boards and chat rooms to find postings of anti-employer comments."

(e) Blogging and the Information Economy

Another timely topic related to employers' online reputations and employees' internet use is blogging. In this information age, employers are scrambling to stay ahead of computing trends. Many are attempting to infiltrate and exploit new forms of digital media, including social networking websites (such as Facebook and LinkedIn), virtual realities (like Second Life) and other web 2.0 technologies.[259] This can result in a 'digital immersion' for employees, who are pushed to find innovative ways to advance the company's interests in these new forums. One consequence of this new business model is that the division between work and personal life will become even more blurred, to the point where it may be non-existent, particularly for employees who are paid a salary (instead of by the hour).[260] In this information economy, a premium is placed on authenticity and credibility, and heavy-handed, autocratic corporate censorship may be the death knell for employer attempts to expand into these new digital realms.[261] As Morgan explains, "[i]n an information economy, employee autonomy is an asset."[262] And further:

---

[259] www.facebook.com; www.linkedin.com; http://secondlife.com. According to the Fortune 500 Business Blogging Wiki, as of May 17, 2008, 58 (or 11.6%) of the Fortune 500 are blogging (*i.e.*, have "active public blogs by company employees about the company and/or its products"): http://www.socialtext.net/bizblogs/.

[260] One recent example is the protest staged by IBM workers in Italy using Second Life, to complain about a performance bonus they had not received: Wency Leung, "STRIKE!* (*banana suit optional)" *The Globe and Mail* (15 October 2007), online: The Globe and Mail <http://www.theglobeandmail.com/servlet/story/RTGAM.20071015.wlunions15/BNStory/lifeWork/home>. See also Evan VanDyk, "Avatars of the World, Unite!" *Slaw* (1 May 2008), online: Slaw <http://www.slaw.ca/2008/05/01/avatars-of-the-world-unite/>.

[261] For an excellent case study, see Michael Barbaro, "Wal-Mart Tastemakers Write Unfiltered Blog" *New York Times* (3 March 2008), online: New York Times <www.nytimes.com/2008/03/03/business/03walmart.html>, which describes the evolution of Wal-Mart's corporate blogging efforts. As he explains, "Several years ago, when the retailer's public relations problems began to mount, it turned to the Web for relief. It created one blog, Working Families for Wal-Mart, to trumpet the chain's accomplishments and ding its critics. It created another, Wal-Marting

> In an information economy, so-called 'Taylorist' business practices are counter-productive. ... Newer business practices, more in keeping with the principles of workplace democracy, place greater responsibility in the hands of employees and downplay the need for heavy surveillance. In such a context, the demands for the respect of personal privacy increase. Widespread efforts at monitoring employees by means of new technology thus seem strangely anachronistic.[263]

As Lifshitz observes, "[b]logging blurs the line between the duty of loyalty that an employee owes to their employer and the personal privacy that an employee is entitled to under common law."[264] The implied terms of the employment contract that are most relevant when it comes to blogging are the employee's duty of loyalty and fidelity, as well as confidentiality.[265] A breach of any of these duties may be cause for discipline; or, depending on the severity of the breach, even termination. There has even been a term coined – "dooced" – for being fired for blogging about one's workplace.[266] Three Canadian doocing cases that have received media attention are Matthew Brown and Starbucks (Toronto); Penny Chomondeley and Nunavut Tourism; and Jeremy Wright and

---

Across America, to highlight the good deeds and productive careers of Wal-Mart employees. Critics dismissed both as thinly veiled extensions of Wal-Mart's P.R. department, and Wal-Mart shut them down." Barbaro describes Wal-Mart's latest blog as one that "turns the traditional model on its head. Instead of relying on polished high-level executives, it is written by little-known buyers, largely without editing."

[262] Morgan, *supra* note 2 at 891.

[263] *Ibid.* at 862. A further discussion of Taylorism in the context of electronic employee monitoring may be found in Uteck, *supra* note 4 at 37-44.

[264] Lifshitz, "Blogging", *supra* note 25 at 89. Relevant statutory privacy protections should also be borne in mind.

[265] *Ibid.* at 92-93.

[266] *Ibid.* at p. 92. See, generally, Sylvia Kierkegaard, "Blogs, Lies and the Doocing: The Next Hotbed of Litigation?" (2006) 22 Computer L. & Sec. R. 127 and Carrie Hoffman, "Employee's Blogging: Protected Activity?" (January 2008), online: Gardere <http://www.gardere.com/Content/hubbard/tbl_s31Publications/FileUpload137/1854/Gardere_Retail_Alert_Doocing.htm>.

Manitoba Health Services.[267] However, to date, none of these individuals have commenced an action for wrongful dismissal against their former employer.[268]

Some of the legal commentary on the topic of blogging features a repetition of the themes raised in connection with more traditional employee uses of computers, internet and e-mail. For example, Lifshitz states, "[i]t seems that it would be even more difficult for an employee to argue that they had a reasonable expectation of privacy in a blog."[269] However, it might be argued that different considerations could apply to onymous versus anonymous blogs; as well, personal blogging efforts might be treated differently than blogs primarily about the workplace (particularly anti-employer blogs). Lifshitz proposes the following list of factors for determining whether an employee has a reasonable expectation of privacy in a blog:

- Existing company policies;
- Practices of fellow employees;
- Whether the employee received any warnings about such behaviour; and
- In some cases, a determination of ownership of the system that was utilized.[270]

As with computer, internet and e-mail usage generally, lawyers recommend that employers put blogging policies into place. Young suggests that any such policy should include the following provisions:

---

[267] For further information on this latter situation, see Jeremy Wright, "I Was Just Fired for Blogging" (5 January 2005), online: Ensight.org <www.ensight.org/archives/2005/01/05/i-was-just-fired-for-blogging/>. The Brown and Wright cases are also discussed by Lee, *supra* note 51 in paras. 21 and 22.
[268] Lifshitz, "Blogging", *supra* note 25 at 92.
[269] *Ibid.* at 91.
[270] *Ibid.* at 90.

- Require compliance with existing codes of conduct and workplace policies;
- Ask employees to use disclaimers, indicating that the views expressed are their own and not their employer's;
- Address confidentiality and non-disclosure; and
- Remind employees not to let blogging interfere with their work.[271]

Young's conclusion reflects a commendable attitude towards employee blogging efforts:

> The policy should be founded on trust, not surveillance or censorship, in promoting responsible blogging. Employee education is the first step. A well-drafted policy can go a long way to educating employees of the potential issues implicated by blogging in or about the workspace, including how it might affect the employment environment, an employer's business reputation and legitimate interests in physical and information security, trade secrets, intellectual property, and a company's obligations under provincial securities regulations.[272]

In this way, blogging may be seen as a microcosm or extension of the law regarding employees' use of computers, internet and e-mail generally.

2. Location Awareness Technologies, Including GPS

In an effort to keep pace with the technologically-enhanced workforce, surveillance itself has become more mobile.[273] As Bennett and Crowe explain, "[t]he workplace is defined less in spatial terms (as a place where all workers have one roof over their heads), but in terms of surveillance. You are in the

---

[271] Young, *supra* note 205 at 10-11.
[272] *Ibid.* at 11.
[273] Colin J. Bennett & Lori Crowe, *Location-Based Services and the Surveillance of Mobility: An Analysis of Privacy Risks in Canada* (June 2005), online: University of Victoria <http://web.uvic.ca/polisci/bennett/pdf/lbsfinal.pdf> [Bennett] at 33.

workplace, where and when your activities can be monitored."[274] The types of workers most susceptible to this type of surveillance are commercial truck drivers, taxi and limousine drivers, couriers and delivery drivers, postal workers, utility technicians and public works employees, along with any other employees whose work involve a great deal of travel or otherwise-unsupervised time outside the physical workplace.[275] Non-mobile workers in more traditional workplace settings (such as office buildings or factories) may also find their locational privacy diminished by the use of swipe cards controlling access to various portions of their workplaces.

Some of the reasons employers implement location awareness technologies have been catalogued by Bennett and Crowe:

> By tracking its mobile workers, companies can increase productivity, save time and expenses, minimize downtime, optimize vehicle utilization, reduce mileage and man hours, secure mobile assets, and reduce mileage costs.[276]

As Levin notes, "...employers seem more receptive to the use of GPS as a productivity measure than they are to the use of the other technologies for this purpose."[277] While employers may monitor employees' computer, internet and e-mail use for the purpose of protecting network security or avoiding legal liability,

---

[274] *Ibid.* at 19.

[275] *Ibid.* at 18. The CBC recently reported that an electronic reminder system has been invented for use in hospitals, to ensure that staff are washing their hands regularly: "Electronic Minder Prompts Handwashing in Hospitals" *CBC News* (3 March 2008), online: CBC News <http://www.cbc.ca/health/story/2008/03/03/handwashing-system.html>. Specific examples of the use of GPS in Canadian workplaces are provided by Treena Hein in "Do you know where your workers are?" *The Globe and Mail* (18 January 2007), online: The Globe and Mail <http://www.theglobeandmail.com/servlet/story/RTGAM.20070118.gttracking18/BNStory/Technology/einsider>. See also *Under the Radar*, *supra* note 14 at 11 and Veilleux, *supra* note 13 at 26. For a discussion of the use of GPS technologies in the United States, see Waseem Karim, "The Privacy Implications of Personal Locators: Why You Should Think Twice Before Voluntarily Availing Yourself to GPS Monitoring" (2004) 14 J.L. & Pol'y 485 and Canoni, *supra* note 59.

[276] Bennett, *ibid.* at 15.

[277] *Under the Radar*, *supra* note 14 at 13.

they are more likely to use GPS data to track employees' performance. It may be that infringing employees' locational privacy is seen as less intrusive than monitoring their personal communications.[278] However, a more stringent test is usually applied where surveillance is used to monitor employees' performance.[279] As well, when it comes to justifying electronic employee monitoring schemes, purely economic motives are always less persuasive than safety or protection of property concerns.[280]

As with computer, internet and e-mail usage, technologies have been developed to counteract location-based electronic employee monitoring.[281] While these technologies may help shield employees' personal activities from employer scrutiny and restore the appropriate balance between commercial concerns and privacy interests, it is questionable whether employees should be required to proactively protect their privacy rights in this manner. It could be argued that if employers wish to implement these types of privacy-invasive technologies, they must also provide employees with the necessary tools for preventing excessive monitoring. For instance, if employees are permitted to use company vehicles for personal purposes after hours, then employers might consider a GPS module that can be turned off in such situations. While this would place the onus on the

---

[278] This seems somewhat counterintuitive, as locational privacy engages two spheres of privacy, whereas personal communications are located wholly within the informational privacy sphere.
[279] Veilleux, *supra* note 13 at 42.
[280] *Ibid.* at 37. Of course, it must be remembered that employment law is heavily influenced by prevailing economic conditions: England, *Individual Employment Law*, *supra* note 68 at 350. Enhanced privacy protections also seem to be the product of a robust economy. When employers are faced with tight profit margins, and their main goal is to maximize profit, this may trigger strict surveillance of and close control over mobile workers and their movements. However, it could also be argued that this type of monitoring is not only motivated by employers' drive for profits, as it may also relate to concerns regarding employee safety or even trustworthiness.
[281] For instance, Cavoukian describes several anti-RFID technologies in *Tag, You're It*, *supra* note 60 at 18-19. Tin-foil hats are not mentioned.

employee, it may also prevent the potential mischief of employees "forgetting" to turn on such GPS units during their working hours. This type of arrangement may come closest to striking the proper balance between employers' and employees' respective interests.

There have not been many employee monitoring cases involving location awareness technologies in Canada to date. One unusual case is that of *Whitehouse v. RBC Dominion Securities Inc*.[282] In that wrongful dismissal action, the employee claimed that he had been dismissed without cause or reasonable notice. He was a vice-president and investment advisor with RBC. The evidence showed that he was one of the company's top-rated investment advisors. Unfortunately, things were not going as well in his private life. After a night of heavy drinking, the employee brought a prostitute back to his office. Apparently this was not the first time he had used his office for such purposes. As described in para. 5 of the decision:

> The Plaintiff used his pass card to enter the building, perhaps forgetting a security camera in the ground floor lobby. He again used his pass card so they could travel by elevator to the office of RBC Dominion Securities Inc. on the 16th floor. ... A card reader report not only marked the precise time of entry - 10:29:48 pm - but also the name of the card owner - James Whitehouse.

After a dispute regarding payment, the employee left the prostitute in the lobby area of the office and took a taxi home. Before taking a taxi herself, the resourceful prostitute left a message on one of the office telephones explaining the situation. In the ensuing investigation, another employee

> ...[V]iewed the card reader report which identified the card used as belonging to the Plaintiff. He viewed the security videotape and

[282] 2006 ABQB 372.

> testified that he saw the Plaintiff and a woman enter an elevator from the ground floor lobby. He listened to the phone message left by [the prostitute].[283]

In the result, the court concluded that the employee's misconduct justified summary dismissal.[284]

Another location-based electronic employee monitoring case is currently winding its way through the Canadian court system. In *Bechthold v. Wendell Motor Sales Ltd.*, the employee quit when his employer sought to install a GPS unit in his company car. He claimed that he was constructively dismissed. His employer maintains that he resigned. At the time of writing, a decision on the merits of the case had not yet been issued.[285]

The federal privacy commissioner's office has issued two findings under PIPEDA that touch on the topic of location-based electronic employee monitoring.[286] The earliest is PIPEDA Case Summary #264, which dealt with both video surveillance and the use of swipe cards in the workplace.[287] In that case, the Assistant Commissioner found that the complaint regarding the photograph-bearing swipe-cards was not well-founded, as the security measures were needed to control access to the facility. However, "inappropriately" showing employee pictures to other staff members (presumably on an otherwise than 'need-to-know' basis) contravened PIPEDA Principle 4.5.

---

[283] Para. 17.
[284] See para. 41.
[285] For a preliminary decision describing the matter, see [2007] O.J. No. 4886 (S.C.J.) (QL).
[286] PIPEDA Case Summary #379, *supra* note 211, discussed above in the context of computer, internet and e-mail monitoring, could arguably also be analogous to location-based electronic employee monitoring scenarios.
[287] *Video cameras and swipe cards in the workplace* (19 February 2004), PIPEDA Case Summary #264, online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040219_01_e.asp>.

The office conducted a thorough review of an employer's implementation of GPS technology in PIPEDA Case Summary #351.[288] As described in the Case Summary:

> Several employees of a telecommunications company complained to the Office when they learned that their employer was installing GPS in their work vehicles. They believed that the company was improperly collecting their personal information, namely their daily movements while on the job. The employees contended that their employer had not obtained their consent to the collection of this information, and that the company had failed to identify the reasons for the collection or state why the information was needed, how it would be used, and how long it would be retained.

Company policy prohibited personal use of these vehicles. The reasons given by the employer for installing these GPS units were "to manage workforce productivity, ensure safety and development, and protect and manage assets...". The technology was going to be linked to an automated dispatch system. The GPS units were capable of capturing "vehicle start and stop times, speed, location, mileage, and off-shift parking location."

The Assistant Commissioner took this opportunity to confirm that data gathered about employees through GPS constituted "personal information" for the purposes of PIPEDA. She applied the following test to determine the appropriateness of GPS in the circumstances:

- Is the measure demonstrably necessary to meet a specific need?
- Is it likely to be effective in meeting that need?
- Is the loss of privacy proportional to the benefit gained?
- Is there a less privacy-invasive way of achieving the same end?[289]

---

[288] *Use of personal information collected by Global Positioning System considered* (9 November 2006), PIPEDA Case Summary #351, online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/cf-dc/2006/351_20061109_e.asp>.

In the result, the Assistant Commissioner accepted the use of GPS for dispatch, safety, and asset protection and management purposes. With respect to employee management, she stated:

> ...[G]iven that the company took measures to limit the use of GPS for such a purpose, would be informing its employees accordingly, and was implementing training to ensure that managers are aware of the appropriate use of the technology, she was satisfied that use of GPS for such a purpose is appropriate in certain limited, exceptional, and defined circumstances, as per subsection 5(3) and Principle 4.8, and that implied consent is present.[290]

The complaint was therefore considered resolved. The Assistant Commissioner's closing comments were summarized as follows:

> In addition to the problems that arise from function creep, the individual's rights are slowly eroded by the cumulative effects of measures intended to meet the bottom line. She cautioned all organizations subject to the Act that **the effects on the dignity of employees of all of the measures in place – taken as a whole, not just as one measure alone – must be considered** in balancing the rights of the individual to privacy and the needs of organizations to collect, use or disclose personal information for appropriate purposes.[291]

Thus, while the use of GPS was found to be acceptable in this particular case, employers must be wary of "function creep" and continually assess the overall impact on employee privacy of all electronic surveillance measures, in addition to any other privacy-invasive workplace policies or procedures.

3. Biometrics

While the topic of biometrics in employment has been generating headlines south of the border, there have not yet been many cases on this topic

---

[289] This is similar to the test adopted by the court in *Eastmond*, *supra* note 128 with respect to video surveillance in the workplace.
[290] PIPEDA Case Summary #351, *supra* note 288.
[291] *Ibid.* [emphasis added].

in Canada. This limited jurisprudence has primarily arisen in connection with unionized workplaces.

There has been some legislation passed regarding the collection, use, retention and disclosure of biometric information. Most of these statutes relate to crossing the border or accessing sensitive undertakings, such as aerodromes and nuclear facilities.[292] The fullest legislative treatment of this subject may be found in articles 44 and 45 of Quebec's *Act to establish a legal framework for information technology*. Article 44 thereof provides as follows:

> *Biometric characteristics.*
> 44. A person's identity may not be verified or confirmed by means of a process that allows biometric characteristics or measurements to be recorded, except with the express consent of the person concerned. Where consent is obtained, only the minimum number of characteristics or measurements needed to link the person to an act and only such characteristics or measurements as may not be recorded without the person's knowledge may be recorded for identification purposes.
>
> *Prohibition.*
> No other information revealed by the characteristics or measurements recorded may be used as a basis for a decision concerning the person or for any other purpose whatsoever. Such information may only be disclosed to the person concerned, at the person's request.
>
> *Records.*
> The record of the characteristics or measurements and any notation relating thereto must be destroyed as soon as the purpose of

[292] On the topic of border-crossing, see *Canadian Passport Order*, S.I./81-86, s. 8.1 and *Presentation of Persons (2003) Regulations*, S.O.R./2003-323, s. 6.3. With respect to aviation, see *Canadian Aviation Security Regulations*, S.O.R./2000-111, ss. 37(2) and 40.2. For access to nuclear facilities, see *Nuclear Security Regulations*, S.O.R./2000-209, s. 17.1 and, more generally, *Employer accused of forcing consent to security screening* (14 August 2002), PIPEDA Case Summary #65, online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/cf-dc/2002/cf-dc_020814_e.asp> and *Should spousal or partner consent be obtained for security clearance checks?* (1 October 2003), PIPEDA Case Summary #232, online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031001_03_e.asp>.

> verification or confirmation of identity has been met or the reason for the verification or confirmation no longer exists.[293]

Article 45 addresses the creation of databases of biometric characteristics and measurements; it provides for mandatory governmental oversight of such initiatives.

The leading case on the use of biometrics in the workplace under PIPEDA is *Wansink v. TELUS Communications Inc*.[294] Telus sought to implement voiceprint technology to permit remote telephonic access by its employees to the company's internal computer network. The biometric aspect of technology was described by the court as follows, in para. 3:

> In order for an employee to use the Nuance Verifier speaker verification technology, the employee must initially participate in an 'enrolment process' that results in the generation of a 'voice template' (or 'voiceprint'). The employee goes through a one-time voice enrolment process where a sample of the voice is taken and a voiceprint is created and stored. Voiceprints are not audio samples but a matrix of numbers that represent the characteristics of the employee's voice and vocal tract. These enrolment voice templates are stored, according to TELUS' evidence, under substantial security for as long as the provider remains an employee of TELUS. Access to e.Speak then requires production of a second voice template which in turn is digitalized and matched against the caller's enrolment voice template. If a match is not obtained, access is denied. This access voice template is destroyed in one or two months.

Four Telus employees filed a complaint under PIPEDA regarding the voiceprint technology. In addition, they alleged that "Telus was threatening them with disciplinary measures for their refusal to submit to voiceprint collection.

[293] R.S.Q. c. C-1.1. These provisions are discussed by Duhaime, *supra* note 57, especially at 18-20.
[294] 2007 FCA 21. See generally Long, *supra* note 133.

Telus has made it known that, for those who fail to enrol, an as yet unspecified form of 'progressive discipline' may be invoked."[295]

The employees' claim failed before the Privacy Commissioner, the Federal Court and the Federal Court of Appeal. The Federal Court of Appeal agreed with the Federal Court judge's comment that "a voice print that is used solely for one-to-one authentication purposes seems to be fairly benign."[296] The use of the technology in the circumstances was found to be reasonable.[297] However, in para. 28, the court held that Telus was obliged to obtain employees' consent before collecting their voice characteristics. Informing employees that a failure to consent could have consequences for their employment did not vitiate their consent.[298] The court made the following comments in paras. 33-34:

> The appellants would like this Court to decide whether Telus' management rights allow it to discipline an employee who refuses to submit personal information protected by PIPEDA.
>
> [34] I will not address this issue. First, TELUS has not taken disciplinary measures which makes answering this question hypothetical. Second, ...[l]abour-law disputes should be settled in a labour-law forum. Once it is found that e.Speak is permissible under PIPEDA and that Telus applies this new technology only to the employees who consent to the collection of their voice characteristics, the employment consequences flowing from the refusal to consent to the reasonable collection of personal information are nowhere to be found in PIPEDA.

It seems reasonable to assume that a similar conclusion would be reached in cases involving individual employment law, that is, that subsidiary employment law issues – including discipline for failing to accept reasonable electronic

[295] Para. 5. It should be noted that the employees were part of a collective bargaining unit.
[296] Paras. 11-12.
[297] Para. 16.
[298] Paras. 29-30.

employee monitoring measures – should not be resolved in the context of a PIPEDA complaint.

York and Carty offer the following conclusion regarding the use of biometrics in the employment context:

> The current state of the law in Canada appears to accept biometric technology in the workplace, as long as it is implemented for a clear business purpose and necessity for its use is supported by objective evidence.[299]

While there have not been many electronic employee monitoring cases involving biometrics in non-unionized workplaces in Canada to date, based on the existing jurisprudence in both unionized and non-unionized workplaces, it appears that York and Carty's conclusion is well-founded.

C. Analogous Jurisprudence

Given the relative novelty of electronic employee monitoring, the relevant case law is still in its infancy. As with most areas of the law, the proper approach to electronic employee monitoring is sought by examining existing jurisprudence on other topics, in the hopes that by finding the best analogy the 'right' legal result will follow.[300] There is undoubtedly a wealth of case law from which such analogies may be drawn, from employee searches to video surveillance and even insubordination or dishonesty.

---

[299] *Supra* note 56 at 26.

[300] Of course, it must be borne in mind that different people have different ideas about what constitutes the "right" result, as this reasoning process is informed by each person's values and ideas and is heavily reliant upon normative judgments. To be clear, this reference is to doctrinal legal reasoning and not necessarily "right" decisions in a normative sense.

Perhaps the most obvious analogy is to the extensive jurisprudence that has developed regarding video surveillance of employees.[301] As Sherrard describes:

> With this approach, the valid business interest of the employer in the integrity of his communication system would be balanced against the privacy rights of the employee. An important similarity between electronic surveillance and video surveillance is the subtle means by which an employer can conduct the surveillance (as opposed, for example, to a body search). … Also, under this model, the employer will have to demonstrate that it had reasonable cause to conduct the search, that the search was carried out in a reasonable manner and that the employer had no other reasonable alternatives at its disposal.[302]

Mitchell and Lewis observe that this analogy is particularly apt, as both video surveillance and electronic monitoring can be either overt or covert.[303] Evidentiary concerns regarding the reliability of information gathered through electronic monitoring are another reason for analogizing such cases with those involving the video surveillance of employees.[304]

In the privacy law context, a four-part test has emerged in video surveillance cases, which was adopted by the Federal Court in *Eastmond*.[305] As Mr. Justice Lemieux stated:

> I am prepared to take into account and be guided by those factors which I repeat are:
>
> - Is camera surveillance and recording necessary to meet a specific [employer] need;

---

[301] Sherrard, *supra* note 35 at 297; Grant Mitchell & David Lewis, "Privacy Issues in the Employment Context" (2004) Pitblado Lect. [Mitchell] at 15; Geist, *supra* note 5 at 173; Poirier, *supra* note 19 at 102; Durnford, *supra* note 24 at 69.
[302] Sherrard, *ibid*. See also Janis Sarra, "Employee Use of E-mail and the Internet: An Arbitrator's Perspective" (2001-2002) 2 Lab. Arb. Y.B. 11 [Sarra] at 24.
[303] Mitchell, *supra* note 301.
[304] Sarra, *supra* note 302 at 24.
[305] *Supra* note 128.

- Is camera surveillance and recording likely to be effective in meeting that need;
- Is the loss of privacy proportional to the benefit gained;
- Is there a less privacy-invasive way of achieving the same end?

> [128] As argued by all parties, these considerations or factors enumerated by the Privacy Commissioner are those which, over the years prior to *PIPEDA*, arbitrators adjudicating privacy issues under collective agreements involving camera surveillance have taken into account in balancing privacy interests of employees with the legitimate interests of employers.

A similar analogy may be drawn to the existing body of law relating to audio surveillance, such as the recording of employees' telephone calls.[306]

Another common analogy in electronic monitoring cases is to searches of employees' lockers or desks.[307] As Sherrard explains:

> If it is reasonable for employees to be protected from a search of their desks and the reading of their personal correspondence, it may be no less reasonable that they be protected if the correspondence is stored on a computer rather than on paper and in a desk drawer. Ownership of the item, in this analysis, becomes irrelevant and it is the employee's expectation of privacy that governs. Following this model, an employer would require reasonable cause to justify the search, would have to conduct the search in a non-discriminatory manner and would have to exhaust other alternatives prior to conducting the search.[308]

It might be said that this analogy is particularly employee-friendly in the electronic monitoring context, as it overcomes the issue of employer property rights and focuses instead on the employees' expectations of privacy. However, some commentators, such as Rasky, argue that electronic monitoring is more akin to a

[306] See e.g. Rasky, *supra* note 20 at 226 and Poirier, *supra* note 19 at 92.
[307] See e.g. Sherrard, *supra* note 35 and Veilleux, *supra* note 13 at 24.
[308] Sherrard, *ibid*.

search of the employer's property. As such, "[t]he rules pertaining to searches of an employee's personal effects should have no application."[309]

In a similar vein, the misuse of corporate internet and e-mail resources may be characterized as insubordination, either (a) based on the substance of the employee's internet postings or e-mail messages or (b) because the employee was previously warned about misusing such facilities.[310] In other cases, employee absorption in personal tasks (like sending and receiving personal e-mails) has been characterized as poor performance and dealt with as such.[311] As well, electronic employee monitoring cases are often linked to the law related to employee dishonesty as many employees, when faced with allegations of misconduct based on employer surveillance efforts, will initially deny any wrongdoing.[312] However, Young suggests that the general law related to employee misconduct is insufficient to address the challenges posed by new technologies, such that new approaches should be adopted and analogies to existing law limited.[313]

As noted above, both employment and workplace privacy laws are heavily influenced by the "rights paradigm". As such, it is not surprising that employees have come to expect certain personal privacy entitlements in the workplace, given the current societal emphasis on individual rights. If privacy is properly characterized as a fundamental human right, then an employer response based

---

[309] Rasky, *supra* note 20 at 223.
[310] See e.g. *Ghattas c. École nationale de théâtre du Canada*, 2006 QCCS 1197 and *Harris, supra* note 229.
[311] See e.g. *Milsom, supra* note 215.
[312] See e.g. *Richardson v. Davis Wire Industries Ltd.* (1997), 28 C.C.E.L. (2d) 101 (B.C.S.C.); *Di Vito*, *supra* note 215; *Bell, supra* note 232.
[313] Young, *supra* note 205 at 10.

on its private property rights will likely fail. It is this re-characterization of employee privacy rights that has allowed them to gain ground. As such, employees seeking to improve their privacy position in the workplace should look to the more general law of human rights to inform and strengthen their arguments. This approach is also reminiscent of civil law notions of privacy, which are based on the inherent dignity of the individual.

IX. *Canada Labour Code* Jurisprudence

A. Introduction to Statutory Unjust Dismissal Schemes

While employment standards legislation provides a minimal amount of protection to dismissed employees, in the form of a statutorily-mandated notice period,[314] if an employee is seeking damages for wrongful dismissal they must generally go to court. However, in three Canadian jurisdictions, the employment standards regime has been enhanced to permit the adjudication of unjust dismissal cases. In Nova Scotia and Quebec, as well as at the federal level, non-unionized employees have access to a neutral adjudicator at the state's expense.[315] In fact, "Nova Scotia was the first Canadian jurisdiction in which legislation was passed prohibiting dismissal outright in the absence of just cause."[316] As England explains, these regimes were put into place in response to

[314] See e.g. *The Employment Standards Code*, S.M. 1998, c. 29, s. 61.
[315] *Labour Standards Code*, R.S.N.S. 1989, c. 246, s. 71; *An Act respecting labour standards,* R.S.Q. c. N-1.1, s. 124; *Canada Labour Code*, R.S.C. 1985, c. L-2, Part III, Division XIV [CLC]. For a full explanation of these provisions, see Geoffrey England, *Unjust Dismissal and Other Termination-Related Provisions* (16 March 2006), online: HRSDC <http://www.hrsdc.gc.ca/en/labour/employment_standards/fls/pdf/research13.pdf> and England & Wood, *supra* note 73, §§17.13-17.214. It should be noted that s. 246(1) of the CLC provides that "No civil remedy of an employee against his employer is suspended or affected" by the unjust dismissal provisions of the CLC.
[316] England & Wood, *ibid.* at §17.203.

the federal government's 1963 ratification of the International Labour Organization's *Termination of Employment Recommendation No. 119*.[317]

In order to file a complaint regarding unjust dismissal under section 240 of the CLC, the following conditions must be met:

> (1) [T]he claimant must qualify as an 'employee,' (2) he or she must not be a 'manager,' (3) he or she must have accrued at least twelve consecutive months of continuous employment with his or her employer, (4) a timely application must have been filed, (5) the claimant must have been dismissed, (6) the claimant must not have been released as a result of a 'layoff,' (7) the claimant must not be covered by a [p. 293] collective agreement or have access to some other statutory procedure for redress, (8) the claimant must have exhausted preadjudication conciliation, and (9) the claimant must have received ministerial approval for adjudication. All of these requirements must be met in order for an adjudicator to have jurisdiction to hear the complaint of unjust dismissal.[318]

Under these laws, the ordinary rules of individual employment law are modified; employees can only be dismissed in limited circumstances. Adjudicators have essentially imported arbitral standards from labour law regarding just cause for dismissal.[319] As England explains:

> To summarize, the notion of just cause in adjudication encompasses the following requirements: the employer must prove that the worker's conduct has caused or is likely to cause substantial harm to the production process, the symbolic legitimacy of management's authority to issue orders, or public confidence in the employer's business; the penalty of dismissal must be proportional to the degree of harm suffered by the employer; appropriate corrective measures must have been followed in dismissals for misconduct and incompetence in order to give the

---

[317] England, *Individual Employment Law*, *supra* note 68 at 291-292. At 292, England observes that "Given the current pressures on Canadian employers to minimize their labour costs in order to compete with foreign firms and on Canadian provincial governments to reduce their debts and deficits, it is unlikely that unjust dismissal schemes will be introduced elsewhere in the near future." The ILO Recommendation is available online at http://www.ilo.org/ilolex/cgi-lex/convde.pl?R119.

[318] England, *Individual Employment Law*, *ibid.* at 292. At 307, England emphasizes that "Compulsory conciliation is the centrepiece of the federal unjust discharge scheme."

[319] *Ibid.* at 307.

> employee a chance to rehabilitate; and any mitigating factors that reduce the severity of the employee's actions must be taken into account.[320]

Different remedies are also available:

> The remedies available to an unjustly dismissed employee under the statutory schemes in the federal jurisdiction, Quebec, and Nova Scotia differ [p. 311] dramatically from the common law position in two key respects. Firstly, compulsory reinstatement is viewed as being the primary remedy for unjust dismissal under the statutory schemes, unlike at common law, where reinstatement is rarely available. Secondly, under the statutory schemes, an unjustly dismissed employee is compensated for the real-world losses flowing from the fact of his or her dismissal, unlike at common law, where damages are limited to contractual entitlements that the employee would have received during the notice period, but not thereafter. This is referred to as the make whole philosophy...[.][321]

Despite these differences, Ball is of the opinion that, particularly with respect to cases involving employees' computer, internet and e-mail use, cases involving individual employment contracts will likely be resolved in the same manner as similar cases under the CLC.[322] Given the usual modality of legal reasoning, this conclusion seems sound.

B. Relevant CLC Cases

There have been a number of CLC cases decided regarding the topics addressed herein.[323] The case of *Goodwin v. Conair Aviation Ltd.* is an excellent

---

[320] *Ibid.* at 308.
[321] *Ibid.* at 310-311. As England notes at 312, "The onus of proving that reinstatement is inappropriate rests with the employer."
[322] Ball, *supra* note 81 at 11:195.
[323] Some of the cases addressed above also arose in the provincial employment standards context, including *Avante*, *supra* note 243; *Daigle*, *supra* note 246; *Boisvert, supra* note 215; *Blais, supra* note 231; and *Gilles, supra* note 215. *Soplet, supra* note 228 was an adjudication decision under the CLC.

starting point.[324] In that case, Ms Goodwin's employment was terminated for four reasons:

> 1. Failure to perform required duties of her position and conducting personal errands on company time;
> 2. Excessive use of telephone and electronic mail for personal use on company time;
> 3. Excessive use of internet for personal use on company time, including live chat lines;
> 4. Failure to be candid and forthright when confronted by the Company respecting the use of the internet, electronic mail, and telephone on company time.[325]

The employer had an Internet and E-mail Policy, but Ms Goodwin was not made aware of it nor was she ever asked sign an Internet and E-mail Agreement. Ms Goodwin had an unblemished employment record with Conair, though she had been counselled informally on several occasions.[326]

In para. 45, Adjudicator Gordon concluded that there was evidence establishing misconduct on the part of Ms Goodwin, showing that she "regularly spent time throughout her work hours, and at times when she was not on her breaks, accessing the internet to retrieve and respond to personal e-mails." In fact, as noted in para. 46:

> Ms. Goodwin admitted in her evidence that she: accessed the internet on a 'regular' basis at least from August 16 to September 12, 2001, mostly for e-mail; used the MSN Messenger program 'occasionally' for chat-line purposes; used the Yahoo service for personal e-mail; and, spent 'some time' on internet/e-mails while not on breaks and when she had company work to do. Ms. Goodwin denied any intentional theft of company time, i.e., intentional claims for pay for work that she did not perform.

[324] 2002 CarswellNat 5265 (Gordon).
[325] Para. 21.
[326] Para. 19.

The adjudicator observed, in para. 47, that "Ms. Goodwin was at work to perform her assigned duties in exchange for her paycheque. She was not at work to conduct personal business during productive time." Nevertheless, the adjudicator decided that Ms Goodwin's conduct was not worthy of summary dismissal. The employer should have used progressive discipline in the circumstances. As such, Ms Goodwin's dismissal was held to be unjust.

In reaching her decision, Adjudicator Gordon relied upon the following extract from "*Employment Law in Canada*, 3rd Edition, Volume II, at paragraph 17.15" regarding section 240 of the CLC:

> The policy of the section derives from I.L.O. Recommendation No. 119, namely *to ensure that the non-unionized employee's personal autonomy and dignity is respected in dismissals*. It is sometimes claimed that the policy of the section is to provide the non-unionized employee with substantially similar protections against unjust dismissal as the unionized employee enjoys under collective agreements. However, it would unduly restrict the broader goal of protecting the employee's personal dignity and autonomy if section 240 were to be viewed as being aimed at merely duplicating collective agreement standards. This is because unions often will be unable to win protections as favourable as those contained in Recommendation No. 119.[327]

If one accepts that the purpose of section 240 of the CLC is to promote the European-inspired ILO policy of respecting employees' personal autonomy and dignity, then it could be argued that greater weight should be given to employees' privacy interests by CLC adjudicators, including in relation to electronic employee monitoring measures.

[327] Para. 28 [Adjudicator Gordon's emphasis].

Another relevant CLC case from 2002 is *Krain v. Toronto-Dominion Bank*.[328] In that case, one of the bank's IT analysts was fired and sought reinstatement to his position under the CLC. He had been employed with the bank for 10 years and had a good service record.[329] An investigation by the bank had determined that Mr. Krain:

- Visited inappropriate Internet sites and downloaded/stored hardcore pornographic information, during business hours using equipment made available to him by the bank.
- Distributed hardcore pornographic information to his personal e-mail account while at work.
- Visited Internet sites for the purpose of acquiring/downloading pirated software, games and movies.
- Copied the software for personal use and sent the pirated software to his personal e-mail account while at work.[330]

Further details regarding the bank's investigation are set out in para. 9, as follows:

> As a result of an audit of the Complainant's Internet use in the early fall of 2001, which appears from the documents to have been prompted by the monitoring of employees with excessive bandwidth consumption (i.e. the level of electronic transmission in a communications network), the Bank determined that between March 12 and June 29, 2001, the Complainant accessed the Internet through his Bank-provided computer to download some 27 messages with 146 different attachments 'of an inappropriate nature'....

The audit also indicated that Mr. Krain downloaded several 'pirated' commercial software applications and that all of this downloading activity occurred during regular working hours.

As noted in para. 5, Mr. Krain admitted that he was aware of the bank's extensive policies regarding computer and internet usage by its employees. He

[328] [2002] C.L.A.D. No. 406 (QL).
[329] Para. 12.
[330] Para. 2.

did not dispute that the bank consistently enforced those policies and that they were reasonable.[331] He admitted that he was guilty of misconduct, but argued that the penalty of summary dismissal was too severe. However, in para. 15, the adjudicator opined as follows:

> While the Bank's written policies permit its employees some latitude for 'web browsing' and even to engage in occasional personal use of the Internet, it also entrusts its employees not to use the Bank's computer to view, download and/or e-mail pornography, unlicensed software, or other materials from obvious inappropriate websites (i.e. sites dedicated to racism, hatred, gambling, etc.). With such latitude must also come some responsibility on the part of the employee to exercise a minimum standard of reasonable judgment in adhering to the justified expectations of the Employer.

And in para. 18:

> Common sense and the Complainant's knowledge as an IT Analyst would have alerted him to the Bank's legitimate security concerns about the importation of unapproved computer programs into its systems, as well as possible civil liability for the illegal use of such programs, which would be reasonably understood by any employee in the Complainant's position to be conduct incompatible with the Bank's necessary institutional reputation for integrity and trust. In many respects, this may be more serious than the private viewing of images of adult nudity and explicit adult sexual conduct, which while inappropriate in the workplace is not illegal per se, whereas the possession and use of unlicensed software exposes the Bank to potential civil liability for copyright infringement.

Echoing the adjudicator's comments in *Goodwin*, *supra*, Adjudicator Luborsky noted in para. 19 that "[t]he Complainant was not hired and did not receive a salary to spend any part of his time in the workplace downloading, viewing and forwarding such images, software programs and games with the Bank's computer resources."

---

[331] Para. 8.

In para. 20, Adjudicator Luborsky concluded that the employee's viewing of sexually explicit materials would not have been sufficient grounds for his dismissal. However, when combined with his downloading of unlicensed software and his distribution of the sexually explicit materials, the adjudicator determined that his dismissal was justified.[332]

Three more CLC cases from 2005 addressed the issue of sexually explicit e-mails and websites. In *C.T. v. Bank of Montreal*,

> [The] Complainant was dismissed by the Bank on April 2, 2003 for storing pornographic e-mails in his inbox at work and forwarding them both internally and externally, misrepresenting his request for an emergency family leave, and making several international long distance calls from a boardroom without authorization and being dishonest about it when interviewed by management.[333]

The employee admitted to using e-mail inappropriately, but argued that dismissal was too harsh a consequence in the circumstances. He also argued that the Bank changed the reason for his termination from inappropriate use of e-mail to dishonesty in an effort to evade its obligation to use progressive discipline.[334] However, there was evidence that the bank's policies regarding computer, internet and e-mail usage were well-known by the employee and had specifically been brought to his attention.

The adjudicator made the following comments regarding the employee's e-mail usage in paras. 66-67:

> C.T. knew, or should have known, that the Bank would monitor the content of e-mail or other internet transmissions when it received a complaint or there was reason to believe that Bank policy had been

[332] In para. 21 the adjudicator specifically noted the reputational concerns that this type of e-mail forwarding posed for the bank.
[333] [2005] C.L.A.D. No. 74 (M.R. Newman) (QL) at para. 1.
[334] Para. 52.

> violated. There should only have been a limited expectation of privacy under those conditions. ...
>
> [67] The record establishes that C.T. received, viewed and retained in his in-box, if not forwarded, data and pictures which may be considered inappropriate or offensive to others. The fact that some may find them to be pornographic, and C.T. did not, is not determinative. Photos with explicit sexual content are not appropriate for either viewing or saving on one's work computer, regardless of whether it is housed in a personal email account. ... By retaining these materials in his in-box, C.T. took the chance that they would be subject to monitoring in the event of a complaint or other reasonable belief of a violation of policy.

In the result, the employee's misuse of his computer, internet and e-mail, coupled with his dishonesty, were found to be sufficient grounds for his termination.

Another relevant CLC case is *Petruccelli v. Canadian National Railway Co*.[335] There, a 25-year CN employee was fired for accessing sexually explicit websites in the workplace. As described in para. 8, "a monthly check by CN's Information Technology Security department in Montreal turned up information that the user of Mr. Petruccelli's computer was accessing pornographic sites." As a result, "[t]he Information Security department sent a computer expert to download on to a disk some of the pornographic images found on Mr. Petruccelli's computer." From that point on, the company continued monitoring Mr. Petruccelli's computer. CN's investigation was described as follows, in para. 18:

> Ms. Lupachow testified that once a month, on no specific day, she makes lists of the first 10 heaviest users of the internet and most frequently visited sites as shown by the number of hits. ... In the process of making up the report for August 2002 she found that the website 'barelylegal.com' had received 468 hits. Suspecting this was a pornography site, she asked Chris Couture, a technician who reported to her, to give her the names of everyone who had

[335] [2005] C.L.A.D. No. 113 (Betcherman) (QL).

> accessed that site. It turned out that all hits came from the user of Mr. Petruccelli's computer. She then went to CN data called 'Webtrends Report' (a minute-by-minute log of activity) for the sites visited by petruc02.cn.ca over the 24-hour period August 15-16. It revealed that the user had visited numerous pornographic sites. She ran Webtrends Reports for other days in August, which confirmed extensive use of Mr. Petruccelli's computer to access pornographic images and material. ... This triggered the downloading of files from Mr. Petruccelli's computer.

However, in the result, the adjudicator sided with Mr. Petruccelli, as progressive discipline was not applied. A three-month unpaid suspension was substituted for his dismissal.

The last of this trio of cases is *Burgess v. Halifax Grain Elevator Ltd*.[336] Mr. Burgess was employed as an Elevator Manager; he was responsible for the operation and maintenance of a grain elevator. The discovery of sexually explicit materials on Mr. Burgess' workplace computer was described as follows, in para. 13:

> The chain of events leading to the termination of Mr. Burgess started in March, 2003 when the computer system of Halifax Grain began to 'slow down'. These difficulties prompted Ms. Juckes to review the personal computers of various employees, including Mr. Burgess, to determine the nature of the problem. On Mr. Burgess's computer she found a large number of 'cookies' indicating that Mr. Burgess had been accessing internet sites. Of particular concern to Ms. Juckes was the nature of the sites involved which contained pornographic material.

The adjudicator confirmed, in para. 84, "that the sites accessed were totally inappropriate and should not, under any circumstances, have been accessed from his employer's computer."

Mr. Burgess was confronted with this information and was warned about his behaviour. As described in paras. 16 and 17:

---

[336] [2005] C.L.A.D. No. 199 (MacPherson).

> Subsequent to this meeting Mr. Burgess did not access pornographic websites at work. For some period of time he did not access any internet sites at all. However, subsequently, during the summer of 2003, he did use the internet, while at work, to access sites concerning recreational four wheel drive vehicles and boats.
>
> [17] Mr. Burgess said that he thought that this type of internet usage was permissible so long as the sites were not 'inappropriate' and other employees had, during working hours, viewed similar types of internet sites.

In fact, Mr. Burgess' supervisor testified that "although the employer's written internet policy provide[d] for 'zero tolerance' in respect of internet usage during working hours, reasonable internet usage by the employees during their lunch hour or before or after work was permitted."[337] Thus, with regard to Mr. Burgess' subsequent, more innocuous internet usage, the adjudicator concluded:

> In any event, even if one assumes that Mr. Burgess viewed these sites during working hours, it appears that his internet usage was similar in nature to the activities of other employees which was permitted by Halifax Grain. Those actions, in and of themselves, would be insufficient to found a termination and would merit, at most, a written warning.[338]

In the result, the adjudicator determined that the employer did not have just cause to terminate Mr. Burgess' employment.

One additional recent case of interest is *Sports Interaction v. Jacobs*.[339] It involved an application for judicial review of the decision of a CLC adjudicator. Therein, an employee was summarily dismissed for comments he made to co-workers using an instant messaging program at work regarding their supervisor and the company. As described in para. 14, "[p]rior to the termination of his employment, the Respondent was an exemplary employee who was never

[337] Para. 19.
[338] Para. 104.
[339] 2007 FC 38, aff'd 2007 FCA 396, leave to appeal denied, [2008] S.C.C.A. No. 47 (QL).

before given a warning, reprimanded or disciplined in any way by his superior or employer."

The adjudicator found that the corporate culture lent itself to the tone of language used by the employee in his instant messages and, furthermore, that there was no company policy regulating or prohibiting the use of instant messaging during working hours.[340] The court's conclusion was as follows:

> I am satisfied that the decision arrived at was reasonably open to the Adjudicator, in that he considered all the evidence, sanctioned the Respondent for his unprofessional and reprehensible behaviour all the while recognizing that the Applicant violated the rules of progressive discipline in its understandable brash first reaction before studied reflection on the contents of the messages. That is why, I am satisfied that the decision of the Adjudicator was not patently unreasonable and should stand. The Application for judicial review is dismissed.[341]

Thus, the employee's termination was found to be unjust, and the four-month suspension substituted by the adjudicator was upheld. This was another case where the employer failed to properly utilize the process of progressive discipline.

X. Comparison to Unionized Workplaces

An exhaustive review of the arbitral jurisprudence that has developed regarding electronic employee monitoring in the context of unionized workplaces in Canada is beyond the scope of this thesis. However, there are four ways in which that substantial body of case law and commentary may be considered relevant to the development of the same law with respect to individual employment relationships.

[340] Para. 37.
[341] Para. 38.

Firstly, and perhaps most importantly, the arbitral jurisprudence regarding electronic employee monitoring brings into sharper focus the tension between individual and collective rights and interests inherent in the workplace privacy debate.[342] Secondly, such cases may provide valuable guidance regarding the resolution of jurisdictional clashes with respect to electronic employee monitoring disputes.[343] Thirdly, the substance of the developed arbitral jurisprudence may assist courts in achieving the optimal balance between employee and employer interests in individual employment law cases involving electronic employee monitoring. This is because there has been considerably more consideration given to the issue of employee privacy in arbitral jurisprudence.[344] Sherrard encourages all employers to be guided by the existing arbitral jurisprudence in this area:

> In order to minimize the negative effects of searching and monitoring employees while effectively protecting legitimate employer interests, all employers (**unionized or not**) are [p. 299] well advised to adhere to the legal principles established by Canadian labour arbitrators.[345]

Lastly, many employment law commentators look wistfully to the law that has developed regarding unionized workplaces and suggest that unionization

---

[342] This concept is briefly touched upon by Veilleux, *supra* note 13 at 20. Of course, one must also avoid the trap of treating the complex, multifaceted issue of electronic employee monitoring as a simple struggle between capital and labour: Mark Jeffery, "Information Technology and Workers' Privacy: The English Law" (2002) 23 Comp. Lab. L. & Pol'y J. 301 at 348. See also Mason, *supra* note 201 at 139 and 148.

[343] See e.g. the leading cases of *Weber v. Ontario Hydro*, [1995] 2 S.C.R. 929 and *Parry Sound (District) Social Services Administration Board v. O.P.S.E.U., Local 324*, [2003] 2 S.C.R. 157.

[344] Ball, *supra* note 81 at 19A:10.

[345] Sherrard, *supra* note 35 298-299 [emphasis added].

would provide employees with the greatest privacy protections.[346] As deBeer explains:

> 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.[347]

Others emphasize that the absence of a collective agreement means that fewer privacy protections are afforded to individual employees.[348] For instance, deBeer notes individual employees' lack of bargaining power vis-à-vis their employers, and so urges that statutory protections be put into place to protect their privacy, as "[n]on-unionized workers cannot be left on their own to bargain for privacy rights."[349]

There are a number of benefits that flow from the way in which the law regarding unionized workplaces is structured, which assist unionized employees in advancing complaints regarding electronic employee monitoring methods. Aside from the increased bargaining power inherent in their numbers and the use of a single collective bargaining agent to negotiate with their employer, two other benefits are inherent in the system. First, employees have the monetary support

---

[346] See e.g. deBeer, *supra* note 3. They may be surprised to find that there are still major gaps remaining in the privacy protections afforded to unionized workers in Canada.
[347] *Ibid.* at 406.
[348] See e.g. Klein, *supra* note 38 at 56-57 and McIsaac, *supra* note 16 at 2.5.4.3(b).
[349] deBeer, *supra* note 3 at 407. See also 384-385, where he writes: "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 [p. 385] privacy."

of the union when pursuing grievances.[350] Second, unions may bring policy grievances on behalf of their members, to challenge any proposed electronic employee monitoring measures before they are implemented. Since individual employees must have recourse to the courts (if they are not protected by unjust dismissal legislation), enforcement of their rights is more costly and it is unlikely that they would keep their jobs while pursuing such actions. As Oscapella explains:

> After all, it takes tremendous energy and courage to fight an employer over a privacy issue. The possible gain – the employer backing away, perhaps only temporarily, from the intrusive behaviour – is hard won, and the potential adverse consequences for the individual worker great, especially if the worker is not backed by a union and the job market is tight. Absent more stringent legal controls on intrusive behaviour by employers, the deck is stacked against workers.[351]

In these ways, unionization provides several procedural benefits to employees disputing electronic monitoring measures, though unionization itself is no guarantee of substantially better privacy protections.

XI. Potential Legislative Reforms

The foregoing survey of the state of the law regarding electronic employee monitoring in Canada reveals that employees are not currently afforded many privacy protections under existing laws. There are therefore numerous avenues to reform that could be explored, namely: (1) employee privacy education campaigns and greater industry self-regulation; (2) enactment of substantially

[350] Of course, this is a double-edged 'benefit'. Given the long-term, political nature of the bargaining process, unions may choose to decline support for one member's grievance (though they must discharge their duty of fair representation) in exchange for a concession benefitting all its members.
[351] Oscapella, *supra* note 3 at 342.

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.

A. 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. 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 latter scenarios currently exists in Canada, it does not appear that greater industry self-regulation will occur in the near future.

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

While it would involve the enactment 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. For instance, Manitoba's Bill 216 borrows heavily from the AB PIPA.[352]

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 which private sector organizations are subject. 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 anticipate and expand to meet future challenges.[353]

---

[352] In the interests of full disclosure, it should be noted that the author was involved with the drafting of Bill 216, *supra* note 135.

[353] A prime example of piecemeal technology-specific legislation is the RFID measures implemented in several American states. 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

The primary difficulty with this approach relates to enforcement. To date, it would appear that an ombudsman-type role has been accepted as appropriate in the context of the access to information regime. This model has been extended to the data protection realm. While accessibility is a mandatory component of any effective privacy protection regime, it is questionable whether the existing ombudsman-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.[354] So long as legislators are unwilling to provide privacy commissioners and their staff with these types of enforcement powers, other (interim) reform measures must be considered.

C. 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.

---

are introduced. While technological developments may require legislative amendment, at least the framework for addressing the new technology would already be clearly established.

[354] This power has been given to the Information and Privacy Commissioners of British Columbia and Alberta, but not the federal Privacy Commissioner: see *supra* notes 169 and 170.

D. 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 which then sets out the exceptions for when surveillance would be considered acceptable. It might even distinguish between covert and overt surveillance. This is the reform approach that has been advocated in Australia.[355]

If such legislation were to be implemented in Canada, useful guidance could be obtained from the existing Australian legislation on this subject.[356] 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

[355] 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).

[356] 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.).

> record geographical location or movement (such as a Global Positioning System tracking device).[357]

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, prohibited surveillance, as well as covert surveillance.

One potential pitfall with this type of legislative reform is that, of those identified herein, it is the most susceptible to losing its technological neutrality. In drafting any such regime, care would have to be taken to keep the definition of surveillance as broad as possible, without being confined 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.

---

[357] *Ibid.*, s. 3.

E. 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. 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 to heart.

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.

XII. Conclusion

Along with the fundamental importance of the employment relationship to individuals, it must be remembered that the employment relationship is ongoing and interdependent.[358] As Sherrard notes, "[i]n the final analysis, employers must keep in mind that positive employee relations are fundamental to maintaining a productive workplace, and that this interest should be at the heart of any decision

[358] Klein, *supra* note 38 at 136.

to conduct...surveillance of employees."[359] Levin goes so far as to say that the protection of workplace privacy is "another form of responsible corporate social conduct" which bolsters the rule of law.[360] Conversely, constant surveillance of employees may undermine, or even supplant, the values of honesty, loyalty and dedication that are at the heart of the employment relationship.[361]

Based on the foregoing review of the current state of Canadian jurisprudence regarding electronic employee monitoring, several suggestions for reform are revealed. 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 for legislative reform in this area are (1) the enactment of private sector privacy laws in all of the provinces of Canada (which may or may not be substantially similar to PIPEDA), which specifically address the topic of electronic employee monitoring;[362] (2) the inclusion of privacy protections in existing employment standards legislation across Canada;[363] or (3) the enactment of stand-alone surveillance legislation. Each of these three potential initiatives has 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

[359] Sherrard, *supra* note 35 at 299.
[360] Levin, "Brother", *supra* note 28 at 228.
[361] Veilleux, *supra* note 13 at 46.
[362] deBeer, *supra* note 3 at 417.
[363] As England observes in his text on *Individual Employment Law*, *supra* note 68 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."

legislation would be primarily focused on the protection of individuals from 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 chosen, 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.[364]

This is another reason why piecemeal technology-specific reforms should be avoided.

If these types of significant reforms are not undertaken, employees may look to unions to collectively bargain for greater privacy protections in the workplace. In the final analysis, employee privacy interests will continue to suffer until some measure of legislative reform is achieved.

[364] Uteck, *supra* note 4 at 183.

XIII. Works Cited

Anderson, Sandra M. “Alberta's Statutory Privacy Regime and Its Impact on the Workplace” (2006) 43 Alta. L. Rev. 647.

Aoki, Cynthia. “Rewriting My Autobiography: The Legal Implications of Memory-Dampening Mechanisms” (The Student “I” Conference, delivered at the University of Ottawa Faculty of Law, 25 October 2007) [unpublished].

Ball, Stacey Reginald. *Canadian Employment Law*, looseleaf (Aurora: Canada Law Book, 1996).

Barbaro, Michael. “Wal-Mart Tastemakers Write Unfiltered Blog” *New York Times* (3 March 2008), online: New York Times <www.nytimes.com/2008/03/03/business/03walmart.html>.

Bennett Colin J. & Lori Crowe. *Location-Based Services and the Surveillance of Mobility: An Analysis of Privacy Risks in Canada* (June 2005), online: University of Victoria <http://web.uvic.ca/polisci/bennett/pdf/lbsfinal.pdf>.

“Borland, Symantec call truce” *CNET* (14 February 1997), online: CNET <http://news.cnet.com/Borland,-Symantec-call-truce/2100-1023_3-271125.html>.

Brunette, Max. “Caught With Their Virtual Pants Down: Can Sending, Receiving and Procuring Offensive Materials from a Workplace Computer Constitute Dismissal for Just Cause?” (2007) 17 E.L.L.R. 69.

Canoni, John D. “Location Awareness Technology and Employee Privacy Rights” (2004) 30 Employee Relations Law Journal 26.

Cavoukian, Ann. “RFID and Privacy: Guidance for Health Care Providers” (2008) 4 Can. Priv. L. Rev. 21.

———. “Technology, Privacy and the Law: The Challenges Ahead” (2006) 7 Internet & E-Commerce Law in Canada 57.

———. *Tag, You’re It: Privacy Implications of Radio Frequency Identification (RFID) Technology* (February 2004), online: Office of the Information and Privacy Commissioner of Ontario <http://www.ipc.on.ca/images/Resources/up-rfid.pdf>.

“Dairy Queen workers’ hijinks on web shock owner” *CBC News* (18 January 2008), online: CBC News <http://www.cbc.ca/consumer/story/2008/01/18/dairy-video.html>.

deBeer, Jeremy. “Employee Privacy: The Need for Comprehensive Protection” (2003) 66 Sask. L. Rev. 383.

Delwaide, Karl & Antoine Aylwin. *Learning from a Decade of Experience: Quebec’s Privacy Sector Privacy Act* (Ottawa: Privacy Commissioner of Canada, 2005).

Duhaime, Lyne. “La protection des renseignements personnels en milieu de travail” (November 2006), online: Fasken Martineau Dumoulin <http://www.fasken.com>.

Durnford, Francis P. “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.

"Electronic Minder Prompts Handwashing in Hospitals" *CBC News* (3 March 2008), online: CBC News <http://www.cbc.ca/health/story/2008/03/03/handwashing-system.html>.

Eltis, Karen. "La surveillance du courrier électronique en milieu de travail: le Québec succombera t-il à l'influence de l'approche américaine?" (2006) 51 McGill L.J. 475.

England, Geoffrey. *Unjust Dismissal and Other Termination-Related Provisions* (16 March 2006), online: HRSDC <http://www.hrsdc.gc.ca/en/labour/employment_standards/fls/pdf/research13.pdf>.

———. *Individual Employment Law* (Toronto: Irwin Law, 2000).

——— & Roderick Wood. *Employment Law in Canada*, 4th ed., looseleaf (Markham: LexisNexis Butterworths, 2005).

Flaherty, David H. "Workplace Surveillance: The Emerging Reality" (1992) Lab. Arb. Y.B. 189.

Ford, Jane. "The Right to Privacy in Employment: A Management Perspective" (1991) 1 Lab. Arb. Y.B. 95.

Geist, Michael A. "Computer and E-mail Workplace Surveillance in Canada: The Shift from Reasonable Expectation of Privacy to Reasonable Surveillance" (2003) 82 Can. Bar Rev. 151.

Goodin, Dan. "Secret Printer ID Codes May Breach EU Privacy Laws" *The Register* (15 February 2008), online: The Register <http://www.theregister.co.uk/2008/02/15/secret_printer_tracking_dots>.

Guillemette, Manon G., Isabelle Fontaine & Claude Caron. “Hybrid RFID-GPS Real-Time Location System for Human Resources: Development, Impacts and Perspectives” (Proceedings of the 41st Hawaii International Conference on System Sciences in Waikoloa, Hawaii, January 2008) <http://csdl2.computer.org/comp/proceedings/hicss/2008/3075/00/30750406.pdf>.

Hein, Treena. “Do you know where your workers are?” *The Globe and Mail* (18 January 2007), online: The Globe and Mail <http://www.theglobeandmail.com/servlet/story/RTGAM.20070118.gttracking18/BNStory/Technology/einsider>.

Hoffman, Carrie. “Employee’s Blogging: Protected Activity?” (January 2008), online: Gardere <http://www.gardere.com/Content/hubbard/tbl_s31Publications/FileUpload137/1854/Gardere_Retail_Alert_Doocing.htm>.

Hope-Tindall, Peter. “Biometrics 101 – An Introduction” (Paper presented in Winnipeg, 11 August 2004) [unpublished].

Ignatieff, Michael. *The Rights Revolution* (Toronto: House of Anansi Press, 2000).

Jeffery, Mark. “Information Technology and Workers’ Privacy: Introduction” (2002) 23 Comp. Lab. L. & Pol’y J. 251.

———. “Information Technology and Workers’ Privacy: The English Law” (2002) 23 Comp. Lab. L. & Pol’y J. 301.

Karim, Waseem. “The Privacy Implications of Personal Locators: Why You Should Think Twice Before Voluntarily Availing Yourself to GPS Monitoring” (2004) 14 J.L. & Pol’y 485.

Kassaris, Eleni. “Employee Personal Information: A Review of Recent Privacy Law Decisions in British Columbia and Alberta” (2007) 17 E.L.L.R. 1.

Kierkegaard, Sylvia. “Blogs, Lies and the Doocing: The Next Hotbed of Litigation?” (2006) 22 Computer L. & Sec. R. 127.

Klein, Kris & Vivian Gates. *Privacy in Employment: Control of Personal Information in the Workplace* (Toronto: Thomson Canada Limited, 2005).

Kosa, James. “Canadian University Challenges Order Regarding Employee Monitoring” *E-Tips* (7 November 2007), online: Deeth Williams Wall <http://www.dww.com/?p=1175#more-1175>.

LaBossiere, Keith D., Karen Clearwater & Scott Hoeppner. “The Nuts and Bolts of Accommodating Employee Privacy” (2007) Pitblado Lect.

Lasprogata, Gail, 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.

Lauzon, Isabelle & Linda Bernier. *La surveillance de vos employés: où, quand, comment?* (Cowansville: Les Éditions Yvon Blais Inc., 2007).

Lawson, Ian & Bill Jeffery. *Privacy and Free Enterprise: The Legal Protection of Personal Information in the Private Sector*, 2nd ed. (Ottawa: Public Interest Advocacy Centre, 1997).

Lee, Konrad. “Anti-Employer Blogging: Employee Breach of the Duty of Loyalty and the Procedure for Allowing Discovery of a Blogger’s Identity Before Service of Process is Effected”, online: (2006) Duke L. & Tech. Rev. 2 <http://www.law.duke.edu/journals/dltr/articles/pdf/2006dltr0002.pdf>.

Leung, Wency. “STRIKE!* (*banana suit optional)” *The Globe and Mail* (15 October 2007), online: The Globe and Mail <http://www.theglobeandmail.com/servlet/story/RTGAM.20071015.wlunions15/BNStory/lifeWork/home>.

Levin, Avner. “Big and Little Brother: The Potential Erosion of Workplace Privacy in Canada” (2007) 22 C.J.L.S. 197.

——— *et al. Under the Radar? The Employer Perspective on Workplace Privacy* (June 2006), online: Ryerson University <http://www.ryerson.ca/tedrogersschool/news/archive/UnderTheRadar.pdf>.

——— & Mary Jo Nicholson. “Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground” (2005) 2 U.O.L.T.J. 357.

Lifshitz, Lisa R. “Corporate Blogging: Navigating Through a Web of Potential Legal Liability – Part I” (2007) 7 Internet & E-Commerce Law in Canada 81.

———. “Corporate Blogging: Navigating Through a Web of Potential Legal Liability – Part II of II” (2007) 7 Internet & E-Commerce Law in Canada 89.

——— & Blair McKechnie. “RFID Technology: Current Legal and Business Considerations - Part 1” (2006) 7 Internet & E-Commerce Law in Canada 25.

Long, Murray. “The Challenge of Employment Consent Under PIPEDA” (2006) 3 Can. Privacy L. Rev. 49.

Mason, David *et al.* “Getting Real about Surveillance and Privacy at Work” in Steve Woolgar, ed., *Virtual Society? Technology, Cyberbole, Reality* (Oxford: Oxford University Press, 2002) 137.

McIsaac, Barbara, Rick Shields & Kris Klein. *The Law of Privacy in Canada*, looseleaf (Scarborough: Carswell, 2000).

Mills, Elinor. “State worker cleared on child porn charges that were due to malware” *CNET* (17 June 2008), online: CNET <http://news.cnet.com/8301-10784_3-9970660-7.html>.

Mitchell, Grant & David Lewis. “Privacy Issues in the Employment Context” (2004) Pitblado Lect.

Morgan, Charles. “Employer Monitoring of Employee Electronic Mail and Internet Use” (1999) 44 McGill L.J. 849.

Morin, Fernand. “Nouvelles technologies et la télésubordination du salarié” (2000) 55 R.I. 725.

Mostrous, Alexi & David Brown. “Microsoft seeks patent for office ‘spy’ software” *The Times* (16 January 2008), online: The Times <http://technology.timesonline.co.uk/tol/news/tech_and_web/article3193480.ece>.

New South Wales Law Reform Commission. *Surveillance: An Interim Report* (Sydney: New South Wales Law Reform Commission, 2001).

Office of the Privacy Commissioner of Canada. News Release, “Lack of basic privacy and security measures causing major data breaches, Privacy Commissioner says” (3 June 2008), online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/media/nr-c/2008/nr-c_080603_e.asp>.

———. “Radio Frequency Identification (RFID) in the Workplace: Recommendations for Good Practices” (March 2008), online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/information/pub/rfid_e.pdf>.

———. “Fact Sheet: RFID Technology” (23 February 2006), online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/fs-fi/02_05_d_28_e.asp>.

Ontario, Ministry of Labour. *Looking Forward: A New Tribunal for Ontario’s Workplaces* (Consultation Paper), February 2001, online: Ontario Ministry of Labour <http://www.ontla.on.ca/library/repository/mon/1000/10293245.pdf>.

Oscapella, Eugene. “Workplace Surveillance: Serving the Omniscient State” (1998) 6 C.L.E.L.J. 341.

Parkes, Debra. “Targeting Workplace Harassment in Quebec: On Exploring a New Legislative Agenda” (2004) 8 Empl. Rts. & Employ. Pol’y 423.

Poirier, Marc-Alexandre. “Employer Monitoring of the Corporate E-mail System: How Much Privacy Can Employees Reasonably Expect?” (2002) 60 U.T. Fac. L. Rev. 85.

Radwanski, George. “Workplace Privacy: A New Act, a New Era” (2001-2002) 2 Lab. Arb. Y.B. 1.

Ramasastry, Anita. “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>.

Rasky, Holly L. “Can an Employer Search the Contents of Its Employees’ E-mail?” (1998) 20 Adv. Q. 221.

Richmond, Lorne A. “Employee Use of E-mail and the Internet: A Union Perspective” (2001-2002) 2 Lab. Arb. Y.B. 45.

Rigg, C.L. “The Right to Privacy in Employment: An Arbitrator's Viewpoint” (1991) 1 Lab. Arb. Y.B. 83.

Sack, Jeffrey *et al.*, eds. “Governments Move to Limit Employees’ Internet Access and E-mail Use” (November/December 2000) 24 *Collective Bargaining Reporter*.

Saint-André, Yves. “Le respect du droit à la vie privée au travail: mythe ou réalité?” in *Développements récents en droit du travail*, Vol. 205 (Cowansville: Les Éditions Yvon Blais Inc., 2004) 51.

Sarra, Janis. “Employee Use of E-mail and the Internet: An Arbitrator's Perspective” (2001-2002) 2 Lab. Arb. Y.B. 11.

Scassa, Teresa *et al. An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies* (28 April

2005), online: Dalhousie University <http://www.library.dal.ca/law/Guides/FacultyPubs/Scassa/RFIDs_Report2(Single).pdf>.

Schafer, Arthur. “Privacy: A Philosophical Overview” in Dale Gibson, ed., *Aspects of Privacy Law: Essays in Honour of John M. Sharp* (Scarborough: Butterworth & Co. (Canada) Ltd., 1980) 1.

Sherrard, Michael G. “Workplace Searches and Surveillance versus the Employee's Right to Privacy” (1999) 48 U.N.B.L.J. 283.

Sookman, Barry B. *Computer, Internet and Electronic Commerce Terms: Judicial, Legislative and Technical Definitions* (Toronto: Thomson Canada Limited, 2007).

Sotto, Lisa J. & Elisabeth M. McCarthy. “An Employer’s Guide to US Workplace Privacy Issues” (2007) 24 The Computer & Internet Lawyer 1.

Spaeth, Juliana M., Mark J. Plotkin & Sandra C. Sheets. “Privacy, Eh!: The Impact of Canada’s *Personal Information Protection and Electronic Documents Act* on Transnational Business” (2002) 4 Vand. J. Ent. L. & Prac. 28.

Taggart, Stewart. “Call It the SyDNA Olympics” *Wired* (7 March 2000), online: Wired <http://www.wired.com/science/discoveries/news/2000/03/34774>.

Uteck, E. Anne. *Electronic Surveillance and Workplace Privacy.* (LL.M. Thesis, Dalhousie University Faculty of Law, 2004) [unpublished].

VanDyk, Evan. “Avatars of the World, Unite!” *Slaw* (1 May 2008), online: Slaw <http://www.slaw.ca/2008/05/01/avatars-of-the-world-unite/>.

———. “Memory” *Slaw* (16 October 2007), online: Slaw <http://www.slaw.ca/2007/10/16/memory/>.

Veilleux, Diane. “Le droit à la vie privée – sa portée face à la surveillance de l’employeur” (2000) 60 R. du B. 1.

Victorian Law Reform Commission. *Workplace Privacy: Final Report* (Melbourne: Victorian Law Reform Commission, 2005).

Wallach, Shelley. “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.

Warren, Samuel & Louis D. Brandeis. “The Right to Privacy” (1890) 4 Harv. L. Rev. 193.

“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>.

Westin, Alan F. *Privacy and Freedom* (New York: Atheneum, 1967).

Willis, E.B. & W.K. Winkler. *Labour Arbitration: The Year in Review 2006* (Aurora: Canada Law Book, 2007).

Wright, Jeremy. “I Was Just Fired for Blogging” (5 January 2005), online: Ensight.org <www.ensight.org/archives/2005/01/05/i-was-just-fired-for-blogging/>.

York, Andrea & Lisa Carty. “Biometrics in the Workplace: Balancing Technology and Privacy” (2006) 16 E.L.L.R. 21.

——— & Bonny Miller. “Privacy in the Ontario Workplace: A Review of the Draft *Privacy of Personal Information Act, 2002*” (2002) 12 E.L.L.R. 25.

Young, Jason. “The Blogger in the Workplace: Considerations for Employers and Employees” (2005) 6 Internet & E-Commerce Law in Canada 9.

XIV. Cases Cited

A. Canadian

Arpin c. Grenier, [2004] J.Q. no 6876 (C.Q. - Petites créances) (QL)

Atwood v. CAC Computers & Communications Inc., 2001 BCSC 875

Aubry v. Éditions Vice-Versa, [1998] 1 S.C.R. 591

Bechthold v. Wendell Motor Sales Ltd., [2007] O.J. No. 4886 (S.C.J.) (QL)

Bell v. Computer Science Corp., 2006 CarswellOnt 9143 (S.C.J.), aff'd 2007 ONCA 466, leave to appeal refused, [2007] S.C.C.A. No. 393 (QL)

Bhamre Employment Insurance Claim Appeal (17 March 1997), CUB 42012A, online: EI <http://www.ei-ae.gc.ca/policy/appeals/cubs/40000-50000/42000-42999/42012AE.html>

Blais c. Société des Loteries Vidéos du Québec Inc., 2003 QCCRT 14

Boisvert c. Industrie Machinex Inc., D.T.E. 2002T-185 (Que. C.T.)

Bongeli v. Citibank Canada, [2004] O.T.C. 686 (S.C.J.), aff'd [2006] O.J. No. 263 (C.A.) (QL)

Burgess v. Halifax Grain Elevator Ltd., [2005] C.L.A.D. No. 199 (MacPherson)

C.T. v. Bank of Montreal, [2005] C.L.A.D. No. 74 (M.R. Newman) (QL)

Condition of Washrooms Prompts Management to Monitor Facilities (4 April 2007), PIPEDA Case Summary #379, online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/cf-dc/2007/379_20070404_e.asp>

Dhoot v. First Calgary Savings & Credit Union, 1998 CarswellAlta 1291 (Q.B.)

Di Vito and Mathers v. Macdonald Dettwiler & Associates Ltd. (1996), 21 C.C.E.L. (2d) 137 (B.C.S.C.)

Eastmond v. Canadian Pacific Railway, 2004 FC 852

Employer accused of forcing consent to security screening (14 August 2002), PIPEDA Case Summary #65, online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/cf-dc/2002/cf-dc_020814_e.asp>

EPCOR Utilities Inc. (10 April 2007), Investigation Report #P2007-IR-004, online: Alberta Information and Privacy Commissioner <http://www.oipc.ab.ca/ims/client/upload/Investigation%20Report%20P2007_IR_004.pdf>

Ferenczy v. MCI Medical Clinics (2004), 70 O.R. (3d) 277 (S.C.J.)

Foerderer v. Nova Chemicals Corp., 2007 ABQB 349

Ghattas c. École nationale de théâtre du Canada, 2006 QCCS 1197

Gilles c. Ciba Spécialités chimiques Canada inc., 2008 QCCRT 134

Goodwin v. Conair Aviation Ltd., 2002 CarswellNat 5265 (Gordon)

Harris Scientific Products Ltd. v. Araujo, 2005 ABQB 603

Hunter v. Southam Inc., [1984] 2 S.C.R. 145

Inform Cycle Ltd. v. Draper, 2008 ABQB 369

Kellogg Brown and Root Canada v. Alberta (Information and Privacy Commissioner), 2007 ABQB 499

Koo Employment Insurance Claim Appeal (10 September 1998), CUB 42710, online: EI <http://www.ei-ae.gc.ca/policy/appeals/CUBs/40000-50000/42000-42999/42710e.html>

Krain v. Toronto-Dominion Bank, [2002] C.L.A.D. No. 406 (QL)

Laval (Société de transport de la Ville de) c. X, [2003] C.A.I. 667

Liberty Smelting Works (1962) Ltd. c. Syndicat international uni de l'automobile, de l'aéroneautique, de l'astronautique et des instrument aratoires d'Amérique (TUA), local 1470, [1972] S.A.G. 1039

Lovelock v. DuPont Canada Inc., [1998] O.J. No. 4971 (Gen. Div.) (QL)

Manchulenko v. Hunterline Trucking Ltd., 2002 BCSC 966

Milsom v. Corporate Computers Inc. (2003), 27 C.C.E.L. (3d) 26 (Alta. Q.B.)

Nesbitt Burns Inc. v. Lange, (2000), 16 C.C.E.L. (3d) 317 (Ont. S.C.J.)

Osiris Inc. v. 1444707 Ontario Ltd., [2005] O.T.C. 1101 (S.C.J.)

Pacific Northwest Herb Corp. v. Thompson, 1999 CarswellBC 2738 (S.C.)

Parkland Regional Library (24 June 2005), Order F2005-003, online: Alberta Information and Privacy Commissioner <http://www.oipc.ab.ca/ims/client/upload/F2005-003.pdf>

Parry Sound (District) Social Services Administration Board v. O.P.S.E.U., Local 324, [2003] 2 S.C.R. 157

Petruccelli v. Canadian National Railway Co., [2005] C.L.A.D. No. 113 (Betcherman) (QL)

Pinto v. BMO Nesbitt Burns Inc. (2005), 40 C.C.E.L. (3d) 293 (Ont. S.C.J.)

Plotogea v. Heartland Appliances Inc. (2007), 60 C.C.E.L. (3d) 216 (Ont. S.C.J.)

Potvin c. Malartic (Ville), 2003 CarswellQue 2093 (C.S.)

Québec (Commission des normes du travail) c. Bourse de Montréal inc., [2002] R.J.Q. 807 (C.S.)

R. v. Dyment, [1988] 2 S.C.R. 417

R. v. McLaughlin, [1980] 2 S.C.R. 331

R. v. Plant, [1993] 3 S.C.R. 281

R. v. Sharpe, [2001] 1 S.C.R. 45

R. v. Tessling, [2004] 3 S.C.R. 432

Re Avante Furniture Manufacturing (1992) Ltd., [2001] B.C.E.S.T.D. No. 64 (QL)

Re Langley Cruiseshipcenters Ltd. (14 December 2006), Order P06-05, online: British Columbia Information and Privacy Commissioner <http://www.oipc.bc.ca/PIPAOrders/2006/OrderP06-05.pdf>

Reference Re Public Service Employee Relations Act (Alta.), [1987] 1 S.C.R. 313

Regina Police Assn. Inc. v. Regina (City) Board of Police Commissioners, [2000] 1 S.C.R. 360

Richardson v. Davis Wire Industries Ltd. (1997), 28 C.C.E.L. (2d) 101 (B.C.S.C.)

Seaton v. Autocars North (1983) Inc. (c.o.b. North Toronto Mazda), [2000] O.T.C. 348 (S.C.J.)

Services d'administration P.C.R. ltée c. Daigle, [2003] J.Q. no 121 (C.S.), aff'd [2003] J.Q. no 4562 (C.A.)

Should spousal or partner consent be obtained for security clearance checks? (1 October 2003), PIPEDA Case Summary #232, online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031001_03_e.asp>

Society of Composers, Authors & Music Publishers of Canada v. Canadian Association of Internet Providers, [2004] 2 S.C.R. 427

Soplet v. Bank of Nova Scotia (2007), 57 C.C.E.L. (3d) 269 (Marvy)

Sports Interaction v. Jacobs, 2007 FC 38, aff'd 2007 FCA 396, leave to appeal denied, [2008] S.C.C.A. No. 47 (QL)

Telecommunications Company Does Not Improperly Collect or Use Employee Statistics (14 April 2003), PIPEDA Case Summary #153, online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030414_3_e.asp>

Thomson Newspapers Ltd. v. Canada (Director of Investigation and Research, Restrictive Trade Practices Commission), [1990] 1 S.C.R. 425

Tremblay c. La Reine, [2003] J.Q. no 5009 (Que. C.A.), leave to appeal denied, [2003] C.S.C.R. no 233 (S.C.C.) (QL)

University of British Columbia (24 September 2007), Order F07-18, online: British Columbia Information and Privacy Commissioner <www.oipc.bc.ca/orders/2007/OrderF07-18.pdf>

Use of personal information collected by Global Positioning System considered (9 November 2006), PIPEDA Case Summary #351, online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/cf-dc/2006/351_20061109_e.asp>

Video cameras and swipe cards in the workplace (19 February 2004), PIPEDA Case Summary #264, online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040219_01_e.asp>.

Wansink v. TELUS Communications Inc., 2007 FCA 21

Weber v. Ontario Hydro, [1995] 2 S.C.R. 929

Whitehouse v. RBC Dominion Securities Inc., 2006 ABQB 372

B. Other (Non-Canadian)

Douglas v. Hello! Ltd., [2007] UKHL 21

Kaye v. Robertson, [1991] FSR 62 (U.K.C.A.)

Lunney v. Prodigy Services Company, 99 N.Y. Int. 0165 (Ct. App. N.Y. December 2, 1999)

Murray v Big Pictures (UK) Ltd., [2008] EWCA Civ 446

Olmstead v. U.S., 277 U.S. 438 (1928)

R. v. Brown, [1996] A.C. 543 (H.L.)

XV. Legislation Cited

A. Canadian

Access to Documents Held by Public Bodies and the Protection of Personal Information, R.S.Q. c. A-2.1, *An Act Respecting*

Access to Information and Protection of Privacy Act, R.S.Y. 2002, c. 1

Access to Information and Protection of Privacy Act, S.N.L. 2002, c. A-1.1

Access to Information and Protection of Privacy Act, S.N.W.T. 1994, c. 20

Canada Labour Code, R.S.C. 1985, c. L-2

Canadian Aviation Security Regulations, S.O.R./2000-111

Canadian Passport Order, S.I./81-86

Charter of Human Rights and Freedoms, R.S.Q., c. C-12

Civil Code of Québec, S.Q. 1991, c. 64

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

Constitution Act, 1982, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11

Consumer Protection Act, C.C.S.M. c. C200, *The*

Criminal Code, R.S.C. 1985, c. C-46

Electronic Commerce Act, 2000, S.O. 2000, c. 17

Electronic Transactions Act, S.A. 2001, c. E-5.5

Employment Standards Code, S.M. 1998, c. 29, *The*

Establish a Legal Framework for Information Technology, R.S.Q. c. C-1.1, *An Act to*

Freedom of Information and Protection of Privacy Act, C.C.S.M. c. F175, *The*

Freedom of Information and Protection of Privacy Act, R.S.A. 2000, c. F-25

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.O. 1990, c. F.31

Freedom of Information and Protection of Privacy Act, R.S.P.E.I. 1988, c. F-15.01

Freedom of Information and Protection of Privacy Act, S.N.S. 1993, c. 5

Freedom of Information and Protection of Privacy Act, S.S. 1990-91, c. F-22.01

Health Information Act, R.S.A. 2000, c. H-5

Health Information Protection Act, S.S. 1999, c. H-0.021

Labour Standards Code, R.S.N.S. 1989, c. 246

Labour Standards, R.S.Q. c. N-1.1, s. 124, *An Act Respecting*

Nuclear Security Regulations, S.O.R./2000-209

Ontario Disability Support Program Act, 1997, S.O. 1997, c. 25, Sch. B

Ontario Works Act, 1997, S.O. 1997, c. 25, Sch. A

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

Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sch. A

Personal Information Protection Act, S.A. 2003, c. P-6.5

Personal Information Protection Act, S.B.C. 2003, c. 63

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5

Personal Information Protection and Identity Theft Prevention Act, Bill 216, 2nd Sess., 39th Leg., Manitoba, 2007, *The*

Personal Investigations Act, R.S.M. 1987, c. P34, *The*

Presentation of Persons (2003) Regulations, S.O.R./2003-323

Privacy Act, R.S.B.C. 1996, c. 373

Privacy Act, R.S.C. 1985, c. P-21

Privacy Act, R.S.M. 1987, c. P125, *The*

Privacy Act, R.S.N. 1990, c. P-22

Privacy Act, R.S.S. 1978, c. P-24

Protection of Personal Information Act, S.N.B. 1998, c. P-19.1

Protection of Personal Information in the Private Sector, R.S.Q., c. P-39.1, *An Act Respecting the*

B. Other (Non-Canadian)

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>

Surveillance Devices Act 1999 (Vic.), as am. by *Surveillance Devices (Workplace Privacy) Act 2006* (Vic.)

Surveillance Devices Act 2007 (N.S.W.)

Workplace Surveillance Act 2005 (N.S.W.)

XVI. Bibliography

Adams, George W. *Canadian Labour Law*, 2nd ed., looseleaf (Aurora: Canada Law Book, 1993).

Adams, Hall, III, Suzanne M. Scheuing & Stacey A. Feeley. "E-mail Monitoring in the Workplace: The Good, the Bad and the Ugly" (2000) 67 Def. Couns. J. 32.

Aiello, John R. "Computer-Based Work Monitoring: Electronic Surveillance and Its Effects" (1993) 23 Journal of Applied Social Psychology 499.

——— & Carol M. Svec. "Computer Monitoring of Work Performance: Extending the Social Facilitation Framework to Electronic Presence" (1993) 23 Journal of Applied Social Psychology 537.

Albert, Russell D. & Karen L. McBean. "Employee Use of E-mail and the Internet: A Management Perspective" (2001-2002) 2 Lab. Arb. Y.B. 33.

Alder, G. Stoney. "Employee Reactions to Electronic Performance Monitoring: A Consequence of Organizational Culture" (2001) 12 Journal of High Technology Management Research 323.

Alge, Bradley J. *et al*. "Information Privacy in Organizations: Empowering Creative and Extrarole Performance" (2006) 91 Journal of Applied Psychology 221.

———, Gary A. Ballinger & Stephen G. Green. "Remote Control: Predictors of Electronic Monitoring Intensity and Secrecy" (2004) 57 Personnel Psychology 377.

Allen, Anita L. *Why Privacy Isn't Everything: Feminist Reflections on Personal Accountability* (Lanham: Rowman and Littlefield, 2003).

———. "The Wanted Gaze: Accountability for Interpersonal Conduct at Work" (2001) 89 Geo. L.J. 2013.

Anandarajan, Murugan & Claire A. Simmers. *Personal Web Usage in the Workplace: A Guide to Effective Human Resources Management* (Hershey: Idea Group Inc., 2004).

Anderson, Sandra M. "Alberta's Statutory Privacy Regime and Its Impact on the Workplace" (2006) 43 Alta. L. Rev. 647.

Anton, Gary & Joseph J. Ward. "Every Breath You Take: Employee Privacy Rights in the Workplace – An Orwellian Prophecy Come True?" (1998) 49 Lab. L.J. 897.

Aoki, Cynthia. "Rewriting My Autobiography: The Legal Implications of Memory-Dampening Mechanisms" (The Student "I" Conference, delivered at the University of Ottawa Faculty of Law, 25 October 2007) [unpublished].

Bainbridge, David I. *Data Protection Law* (Welwyn Garden City: CLT Professional Publishing, 2000).

Ball, Stacey Reginald. *Canadian Employment Law*, looseleaf (Aurora: Canada Law Book, 1996).

Barbaro, Michael. "Wal-Mart Tastemakers Write Unfiltered Blog" *New York Times* (3 March 2008), online: New York Times <www.nytimes.com/2008/03/03/business/03walmart.html>.

Barss, Allan. “Search and Surveillance in the Workplace: The Employee's Perspective” (1992) Lab. Arb. Y.B. 181.

Bennett Colin J. & Lori Crowe. *Location-Based Services and the Surveillance of Mobility: An Analysis of Privacy Risks in Canada* (June 2005), online: University of Victoria <http://web.uvic.ca/polisci/bennett/pdf/lbsfinal.pdf>.

Bennett, Steven C. & Scott D. Locke. “Privacy in the Workplace: A Practical Primer” (1998) 49 Lab. L.J. 781.

Bernstein, Anita. “What We Talk About When We Talk About Workplace Privacy” (2006) 66 La. L. Rev. 923.

Bevan, Lynn & Andrew Staniusz. “Search and Surveillance in the Workplace: The Employer's Perspective” (1992) Lab. Arb. Y.B. 165.

Beyond Four Walls and a Door: Understanding Privacy in the Office (Zeeland: Herman Miller, Inc., 1990).

Bilson, Beth. “Search and Surveillance in the Workplace: An Arbitrator's Perspective” (1992) Lab. Arb. Y.B. 143.

Block, Jerald J. “Issues for DSM-V: Internet Addiction” (2008) 165 Am. J. Psychiatry 306.

“Borland, Symantec call truce” *CNET* (14 February 1997), online: CNET <http://news.cnet.com/Borland,-Symantec-call-truce/2100-1023_3-271125.html>.

Breckenridge, Adam Carlyle. *The Right to Privacy* (Lincoln: University of Nebraska Press, 1970).

Brown, Donald J. M. & David M. Beatty. *Canadian Labour Arbitration*, 4th ed., looseleaf (Aurora: Canada Law Book, 2006).

Brown, William S. “Ontological Security, Existential Anxiety and Workplace Privacy” (2000) 23 Journal of Business Ethics 61.

———. “Technology, Workplace Privacy and Personhood” (1996) 15 Journal of Business Ethics 1237.

Brunette, Max. “Caught With Their Virtual Pants Down: Can Sending, Receiving and Procuring Offensive Materials from a Workplace Computer Constitute Dismissal for Just Cause?” (2007) 17 E.L.L.R. 69.

Bullock, Jessica A. & Jennifer A. Harker. “Disclosure of Personal Employee Information in the Unionized Workplace” (2006) 16 E.L.L.R. 79.

Burns, Peter. “The Law and Privacy: The Canadian Experience” (1976) 54 Can. Bar Rev. 1.

Butler, Barbara. *Alcohol and Drugs in the Workplace* (Toronto: Butterworths Canada Ltd., 1993).

Canoni, John D. “Location Awareness Technology and Employee Privacy Rights” (2004) 30 Employee Relations Law Journal 26.

Casey, James T. & Leah M. Fitzgerald. “Monitoring Employees at Work: An Arbitrator’s Perspective” (2007 Labour Arbitration and Policy Conference Calgary, 13-14 June 2007) [unpublished].

Cate, Fred H. *Privacy in the Information Age* (Washington: Brookings Institution Press, 1997).

Cavoukian, Ann. “RFID and Privacy: Guidance for Health Care Providers” (2008) 4 Can. Priv. L. Rev. 21.

———. “Technology, Privacy and the Law: The Challenges Ahead” (2006) 7 Internet & E-Commerce Law in Canada 57.

———. *Tag, You’re It: Privacy Implications of Radio Frequency Identification (RFID) Technology* (February 2004), online: Office of the Information and Privacy Commissioner of Ontario <http://www.ipc.on.ca/images/Resources/up-rfid.pdf>.

Charnetski, William, Patrick Flaherty & Jeremy Robinson. *The Personal Information Protection and Electronic Documents Act: A Comprehensive Guide* (Aurora: Canada Law Book Inc., 2001).

Chester, Simon. “PIPEDA Reference Raises Vital Constitutional Questions” (2004) 1 Can. Priv. Law Rev. 52.

Cohen, Cynthia F. & Murray E. Cohen. “On-duty and Off-duty: Employee Right to Privacy and Employer’s Right to Control in the Private Sector” (2007) 19 Employ. Respons. Rights J. 235.

Conlon, Kevin J. “Privacy in the Workplace” (1996) 72 Chicago-Kent L. Rev. 285.

Craver, Charles B. “Privacy Issues Affecting Employers, Employees, and Labor Organizations” (2006) 66 La. L. Rev. 1057.

Cvrcek, Dan *et al*. “A Study on the Value of Location Privacy” (5th Association for Computing Machinery Workshop on Privacy in Electronic Society) (New York: ACM Press, 2006).

"Dairy Queen workers' hijinks on web shock owner" *CBC News* (18 January 2008), online: CBC News <http://www.cbc.ca/consumer/story/2008/01/18/dairy-video.html>.

David, Ira. "Privacy Concerns Regarding the Monitoring of Instant Messaging in the Workplace: Is it Big Brother or Just Business?" (2004) 5 Nev. L.J. 319.

deBeer, Jeremy. "Employee Privacy: The Need for Comprehensive Protection" (2003) 66 Sask. L. Rev. 383.

Delwaide, Karl & Antoine Aylwin. *Learning from a Decade of Experience: Quebec's Privacy Sector Privacy Act* (Ottawa: Privacy Commissioner of Canada, 2005).

Dionisopoulos, P. Allan & Craig R. Ducat. *The Right to Privacy: Essays and Cases* (St. Paul: West Publishing Co., 1976).

Drapeau, Michel W. & Marc-Aurèle Racicot. *Federal Access to Information and Privacy Legislation Annotated 2007* (Toronto: Thomson Canada Limited, 2006).

——— & Marc-Aurèle Racicot. *Protection of Privacy in the Canadian Private and Health Sectors* (Scarborough: Thomson Canada Limited, 2006).

Duffy, Francis. *The Changing Workplace* (London: Phaidon Press Limited, 1992).

Duhaime, Lyne. "La protection des renseignements personnels en milieu de travail" (November 2006), online: Fasken Martineau Dumoulin <http://www.fasken.com>.

Durnford, Francis P. “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.

D’Urso, Scott. “Who’s Watching Us at Work? Toward a Structural-Perceptual model of Electronic Monitoring and Surveillance in Organizations” (2006) 16 Communication Theory 281.

Edwards, Jennifer J. *Human Resources Guide to Workplace Privacy* (Aurora: Aurora Professional Press, 2003).

“Electronic Minder Prompts Handwashing in Hospitals” *CBC News* (3 March 2008), online: CBC News <http://www.cbc.ca/health/story/2008/03/03/handwashing-system.html>.

Eltis, Karen. “La surveillance du courrier électronique en milieu de travail: le Québec succombera t-il à l'influence de l'approche américaine?” (2006) 51 McGill L.J. 475.

———. “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.

England, Geoffrey. *Unjust Dismissal and Other Termination-Related Provisions* (16 March 2006), online: HRSDC <http://www.hrsdc.gc.ca/en/labour/employment_standards/fls/pdf/research13.pdf>.

———. *Individual Employment Law* (Toronto: Irwin Law, 2000).

——— & Roderick Wood. *Employment Law in Canada*, 4th ed., looseleaf (Markham: LexisNexis Butterworths, 2005).

Fairweather, N. Ben. “Surveillance in Employment: The Case of Teleworking” (1999) 22 Journal of Business Ethics 39.

Fenner, Deborah B., F. Javier Lerch & Carol T. Kulik. “The Impact of Computerized Performance Monitoring and Prior Performance Knowledge on Performance Evaluation” (1993) 23 Journal of Applied Social Psychology 573.

Finkin, Matthew W. “Life Away From Work” (2006) 66 La. L. Rev. 945.

———. “Employee Privacy, American Values, and the Law” (1996) 72 Chicago-Kent L. Rev. 221.

Fisk, Catherine L. “Privacy, Power, and Humiliation at Work: Re-Examining Appearance Regulation as an Invasion of Privacy” (2006) 66 La. L. Rev. 1111.

Flaherty, David H. “Workplace Surveillance: The Emerging Reality” (1992) Lab. Arb. Y.B. 189.

———. *Protecting Privacy in Surveillance Societies: the Federal Republic of Germany, Sweden, France, Canada, and the United States* (Chapel Hill: University of North Carolina Press, 1989).

Ford, Jane. “The Right to Privacy in Employment: A Management Perspective” (1991) 1 Lab. Arb. Y.B. 95.

Foucault, Michel. *Discipline and Punish: The Birth of the Prison*, trans by. Alan Sheridan (London: Penguin Books Ltd., 1977).

Friedman, Barry A. & Lisa J. Reed. “Workplace Privacy: Employee Relations and Legal Implications of Monitoring Employee E-mail Use” (2007) 19 Employ. Respons. Rights J. 75.

Geist, Michael A. “In Defence of PIPEDA” (2004) 1 Can. Priv. Law Rev. 55.

———. “Computer and E-mail Workplace Surveillance in Canada: The Shift from Reasonable Expectation of Privacy to Reasonable Surveillance” (2003) 82 Can. Bar Rev. 151.

Gely, Rafael & Leonard Bierman. “Workplace Blogs and Workers’ Privacy” (2006) 66 La. L. Rev. 1079.

Giles, Duncan. “New Australian Right to Protection from ‘Highly Offensive’ Invasions of Privacy” (2003) 1 Can. Privacy L. Rev. 7.

Glenn, H. Patrick. “Le droit au respect de la vie privée” (1979) 39 R. du B. 879.

Goodin, Dan. “Secret Printer ID Codes May Breach EU Privacy Laws” *The Register* (15 February 2008), online: The Register <http://www.theregister.co.uk/2008/02/15/secret_printer_tracking_dots>.

Gordon, Sheldon. “The New Rules of Workplace Privacy” (June 2003) 12:4 Nat. (C.B.A.) 34.

Gormley, Ken. “One Hundred Years of Privacy” (1992) Wis. L. Rev. 1335.

Gorsky, Morley R., S.J. Uprich & Gregory J. Brandt. *Evidence and Procedure in Canadian Labour Arbitration*, 2nd ed., looseleaf (Toronto: Thomson Canada Limited, 1994).

Griffith, Terri L. “Monitoring and Performance: A Comparison of Computer and Supervisor Monitoring” (1993) 23 Journal of Applied Social Psychology 549.

Guillemette, Manon G., Isabelle Fontaine & Claude Caron. “Hybrid RFID-GPS Real-Time Location System for Human Resources: Development, Impacts and Perspectives” (Proceedings of the 41st Hawaii International Conference on System Sciences in Waikoloa, Hawaii, January 2008) <http://csdl2.computer.org/comp/proceedings/hicss/2008/3075/00/30750406.pdf>.

Gunasekara, Gehan. “The ‘Final’ Privacy Frontier? Regulating Trans-border Data Flows” (2006) 15 Int’l J.L. & I.T. 362.

Haggerty, Kevin D. & Richard V. Ericson, eds. *The New Politics of Surveillance and Visibility* (Toronto: University of Toronto Press, 2006).

Heath, Mark E. “A Work Place Surveillance: Who’s Watching?” (2002) 16 J. Nat. Resources & Envtl. L. 59.

Hein, Treena. “Do you know where your workers are?” *The Globe and Mail* (18 January 2007), online: The Globe and Mail <http://www.theglobeandmail.com/servlet/story/RTGAM.20070118.gttracking18/BNStory/Technology/einsider>.

Hewitt, Patricia. *Privacy Report* (Chesham: Robendene Ltd., 1977).

Higgins, Tracy E. “Reviving the Public/Private Distinction in Feminist Theorizing” (2000) 75 Chicago-Kent L. Rev. 847.

Hodges, Ann C. “Bargaining for Privacy in the Unionized Workplace” (2006) 22 Int’l J. Comp. Lab. L. & Ind. Rel. 147.

Hoffman, Carrie. “Employee’s Blogging: Protected Activity?” (January 2008), online: Gardere <http://www.gardere.com/Content/hubbard/tbl_s31Publications/FileUpload137/1854/Gardere_Retail_Alert_Doocing.htm>.

Hooper, Carey C. “‘You’ve Got Mail’: Privacy Rights in the Workplace” (2001) 25 S. Ill. U.L.J. 609.

Hope-Tindall, Peter. “Biometrics 101 – An Introduction” (Paper presented in Winnipeg, 11 August 2004) [unpublished].

Hubbartt, William S. *The New Battle Over Workplace Privacy* (New York: AMACOM, 1998).

Ignatieff, Michael. *The Rights Revolution* (Toronto: House of Anansi Press, 2000).

Information and Privacy Commissioner of Ontario. *Tag, You’re It: Privacy Implications of Radio Frequency Identification (RFID) Technology* by Ann Cavoukian (February 2004) <http://www.ipc.on.ca/images/Resources/up-rfid.pdf>.

Jeffery, Mark. “Information Technology and Workers’ Privacy: Introduction” (2002) 23 Comp. Lab. L. & Pol’y J. 251.

———. “Information Technology and Workers’ Privacy: The English Law” (2002) 23 Comp. Lab. L. & Pol’y J. 301.

Jolls, Christine. “Employment Law and the Labor Market” (2007) online: National Bureau of Economic Research <http://www.nber.org/papers/w13230>.

Jordan, Donald J. “Use of an Employer's E-mail System: Is There a Reasonable Expectation of Privacy?” (1999) 9 E.L.L.R. 92.

Kainen, Burton & Shel D. Myers. “Turning Off the Power on Employees: Using Surreptitious Tape-Recordings and E-mail Intrusions by Employees in Pursuit of Employer Rights” (1997) 48 Lab. L.J. 199.

Karim, Waseem. “The Privacy Implications of Personal Locators: Why You Should Think Twice Before Voluntarily Availing Yourself to GPS Monitoring” (2004) 14 J.L. & Pol’y 485.

Kassaris, Eleni. “Employee Personal Information: A Review of Recent Privacy Law Decisions in British Columbia and Alberta” (2007) 17 E.L.L.R. 1.

Kierkegaard, Sylvia. “Blogs, Lies and the Doocing: The Next Hotbed of Litigation?” (2006) 22 Computer L. & Sec. R. 127.

Kim, Pauline T. “Collective and Individual Approaches to Protecting Employee Privacy: The Experience with Workplace Drug Testing” (2006) 66 La. L. Rev. 1009.

Kiss, Simon & Vincent Mosco. “Negotiating Electronic Surveillance in the Workplace: A Study of Collective Agreements in Canada” (2005) 30 Canadian Journal of Communication 549.

Kleeman, Walter B., Jr. *et al. Interior Design of the Electronic Office: The Comfort and Productivity Payoff* (New York: Van Nostrand Reinhold, 1991).

Klein, Kris & Vivian Gates. *Privacy in Employment: Control of Personal Information in the Workplace* (Toronto: Thomson Canada Limited, 2005).

Knight, Jamie, Sharon Chilcott & Melanie McNaught. *Canada Personal Information Protection and Electronic Documents Act: Quick Reference* (Toronto: Thomson Canada Limited, 2005).

Kosa, James. "Canadian University Challenges Order Regarding Employee Monitoring" *E-Tips* (7 November 2007), online: Deeth Williams Wall <http://www.dww.com/?p=1175#more-1175>.

Kupritz, Virginia W. "Privacy in the Work Place: The Impact of Building Design" (1998) 18 Journal of Environmental Psychology 341.

LaBossiere, Keith D., Karen Clearwater & Scott Hoeppner. "The Nuts and Bolts of Accommodating Employee Privacy" (2007) Pitblado Lect.

Laperrière, René & Nicole Kean. "Le droit des travailleurs au respect de leur vie privée" (1994) 35 C. de D. 709.

Lasprogata, Gail, 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.

Lauzon, Isabelle & Linda Bernier. *La surveillance de vos employés: où, quand, comment?* (Cowansville: Les Éditions Yvon Blais Inc., 2007).

Lawson, Ian & Bill Jeffery. *Privacy and Free Enterprise: The Legal Protection of Personal Information in the Private Sector*, 2nd ed. (Ottawa: Public Interest Advocacy Centre, 1997).

Lee, Konrad. "Anti-Employer Blogging: Employee Breach of the Duty of Loyalty and the Procedure for Allowing Discovery of a Blogger's Identity Before

Service of Process is Effected", online: (2006) Duke L. & Tech. Rev. 2 <http://www.law.duke.edu/journals/dltr/articles/pdf/2006dltr0002.pdf>.

Leung, Wency. "STRIKE!* (*banana suit optional)" *The Globe and Mail* (15 October 2007), online: The Globe and Mail <http://www.theglobeandmail.com/servlet/story/RTGAM.20071015.wlunions15/BNStory/lifeWork/home>.

Lever, Annabelle. "Feminism, Democracy and the Right to Privacy" online: (2005) 9 Minerva 1 <http://www.ul.ie/~philos/vol9/Feminism.html>.

Levin, Avner. "Big and Little Brother: The Potential Erosion of Workplace Privacy in Canada" (2007) 22 C.J.L.S. 197.

———. "Is Workplace Surveillance Legal in Canada?" (2007) 6 Int. J. Inf. Secur. 313.

——— *et al. Under the Radar? The Employer Perspective on Workplace Privacy* (June 2006), online: Ryerson University <http://www.ryerson.ca/tedrogersschool/news/archive/UnderTheRadar.pdf>.

——— & Mary Jo Nicholson. "Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground" (2005) 2 U.O.L.T.J. 357.

Lifshitz, Lisa R. "Corporate Blogging: Navigating Through a Web of Potential Legal Liability – Part I" (2007) 7 Internet & E-Commerce Law in Canada 81.

———. "Corporate Blogging: Navigating Through a Web of Potential Legal Liability – Part II of II" (2007) 7 Internet & E-Commerce Law in Canada 89.

——— & Blair McKechnie. “RFID Technology: Current Legal and Business Considerations - Part 1” (2006) 7 Internet & E-Commerce Law in Canada 25.

——— & Blair McKechnie. “RFID Technology: Current Legal and Business Considerations - Part 2” (2006) 7 Internet & E-Commerce Law in Canada 33.

Linowes, David F. *Privacy in America: Is Your Private Life in the Public Eye?* (Chicago: University of Illinois, 1989).

Loch, Karen D., Sue Conger & Effy Oz. “Ownership, Privacy and Monitoring in the Workplace: A Debate on Technology and Ethics” (1998) 17 Journal of Business Ethics 653.

Long, Murray. “The Challenge of Employment Consent Under PIPEDA” (2006) 3 Can. Privacy L. Rev. 49.

Loukidelis, David. “Privacy Laws in the Workplace - Do the New Privacy Laws Make a Difference?” (Insight Conference on Human Resources Management in a Hot Economic Climate, delivered in Vancouver, 28 November 28, 2006) <http://www.oipcbc.org/publications/speeches_presentations/Privacy_Workplace(InsightVancouver)(28Nov06).pdf>.

———. “Arbitrators & Privacy Commissioners – Why They Should Listen to Each Other” (Insight Conference on Privacy Laws and Effective Workplace Investigations, delivered in Calgary, May 2004) <http://www.oipcbc.org/publications/speeches_presentations/workplace_privacy.pdf>.

Lyon, David. *Surveillance Studies: An Overview* (Malden: Polity Press, 2007).

———. *Surveillance Society: Monitoring Everyday Life* (Philadelphia: Open University Press, 2001).

——— & Elia Zureik, eds. *Computers, Surveillance & Privacy* (Minneapolis: University of Minnesota Press, 1996).

Majzub, Diba. "Employee Privacy: A Critical Examination of the *Doman* Decision" (1998) 4 Appeal 72.

Maltby, L.L. "Workplace Electronic Monitoring" (1993) 6 E.L.L.R. 66.

Mann, Jane. "Privacy at Work in the United Kingdom" (2002) 30 Int'l Bus. Law. 150.

Manning, Rita C. "Liberal and Communitarian Defenses of Workplace Privacy" (1997) 16 Journal of Business Ethics 817.

Marx, Gary T. "Ethics for the New Surveillance" in Colin J. Bennett & Rebecca Grant, eds., *Visions of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999).

Matthews, Jamie L. "Employee Has Invasion of Privacy Claim for Being Terminated After Smoking Cigarettes Off-the-Job" (7 February 2008), online: Foley Hoag LLP <http://www.foleyhoag.com/NewsCenter/Publications/Alerts/Employment-Bulletin/Employment-Bulletin-020708.aspx>.

McGowan, Don. "Québec Challenges Constitutionality of PIPEDA" (2004) 1 Can. Priv. Law Rev. 47.

McIsaac, Barbara, Rick Shields & Kris Klein. *The Law of Privacy in Canada*, looseleaf (Scarborough: Carswell, 2000).

McKay-Panos, Linda. "Workplace: Surveillance" (2007) 32 LawNow 31.

McNairn, Colin H.H. & Alexander K. Scott. *A Guide to the Personal Information Protection and Electronic Documents Act* (Markham: LexisNexis Canada Inc., 2005).

——— & Alexander K. Scott. *Privacy Law in Canada* (Toronto: Butterworths, 2001).

McNall, Laurel A. & Sylvia G. Roch. "Effects of Electronic Monitoring Types of Perceptions of Procedural Justice, Interpersonal Justice, and Privacy" (2007) 37 Journal of Applied Social Psychology 658.

McNaughton, Elizabeth & Andrea York. "New Protection for Employees' Personal Information: An Employer's Introduction to *PIPEDA*" (2001) 11 E.L.L.R. 42.

Mignin, Robert J., Bart A. Lazar & Josh M. Friedman. *Privacy Issues in the Workplace: A Post-September 11 Perspective* (2002) 28 Employee Relations Law Journal 7.

Miller, Seumas & John Weckert. "Privacy, the Workplace and the Internet" (2000) 28 Journal of Business Ethics 255.

Mills, Elinor. "State worker cleared on child porn charges that were due to malware" *CNET* (17 June 2008), online: CNET <http://news.cnet.com/8301-10784_3-9970660-7.html>.

Mitchell, Grant & David Lewis. "Privacy Issues in the Employment Context" (2004) Pitblado Lect.

Mitchnick, Morton & Brian Etherington. *Labour Arbitration in Canada* (Toronto: Lancaster House, 2006).

Monahan, Torin, ed. *Surveillance and Security: Technological Politics and Power in Everyday Life* (New York: Routledge, 2006).

Moore, Adam D. "Employee Monitoring: Evaluative Surveillance v. Privacy" in Adam D. Moore, ed., *Information Ethics: Privacy, Property, and Power* (Seattle: University of Washington Press, 2005).

Moore, Barrington. *Privacy: Studies in Social and Cultural History* (Armonk, N.Y.: Pantheon Books, 1984).

Morgan, Charles. "Employer Monitoring of Employee Electronic Mail and Internet Use" (1999) 44 McGill L.J. 849.

Morin, Fernand. "Nouvelles technologies et la télésubordination du salarié" (2000) 55 R.I. 725.

Mostrous, Alexi & David Brown. "Microsoft seeks patent for office 'spy' software" *The Times* (16 January 2008), online: The Times <http://technology.timesonline.co.uk/tol/news/tech_and_web/article3193480.ece>.

Nebeker, Delbert M. & B. Charles Tatum. "The Effects of Computer Monitoring, Standards, and Rewards on Work Performance, Job Satisfaction, and Stress" (1993) 23 Journal of Applied Social Psychology 508.

New South Wales Law Reform Commission. *Surveillance: An Interim Report* (Sydney: New South Wales Law Reform Commission, 2001).

———. *Surveillance: Final Report* (Sydney: New South Wales Law Reform Commission, 2005).

Nichols, Donald H. “Window Peeping in the Workplace: A Look into Employee Privacy in a Technological Era” (2001) 27 Wm. Mitchell L. Rev. 1587.

Nissenbaum, Helen. “Privacy as Contextual Integrity” (2004) 79 Wash. L. Rev. 101.

Novakowski, Lorene & Karla Koles. *Personal Information Protection Act, British Columbia and Alberta: Quick Reference* (Toronto: Thomson Canada Limited, 2007).

Office of the Privacy Commissioner of Canada. “Radio Frequency Identification (RFID) in the Workplace: Recommendations for Good Practices” (March 2008), online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/information/pub/rfid_e.pdf>.

———. “Fact Sheet: RFID Technology” (23 February 2006), online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/fs-fi/02_05_d_28_e.asp>.

———. *Your Privacy Responsibilities - Canada's Personal Information Protection and Electronic Documents Act: A Guide for Businesses and Organizations* (Ottawa: Office of the Privacy Commissioner of Canada, 2004).

Ontario Bar Association. *The Absolute Very Latest Up to the Minute News, Tips and Strategies in Privacy Law and Compliance* (May 5, 2003).

O'Reilly, John C. *An Employer's Guide to Surveillance, Searches and Medical Examinations* (Toronto: Thomson Canada Limited, 2003).

O'Rourke, Anne, Amanda Pyman & Julian Teicher. "The Right to Privacy and the Conceptualisation of the Person in the Workplace: A Comparative Examination of EU, US and Australian Approaches" (2007) 23 Int'l. J. Comp. Lab. L. & Ind. Rel. 161.

Oscapella, Eugene. "Workplace Surveillance: Serving the Omniscient State" (1998) 6 C.L.E.L.J. 341.

Parkes, Debra. "Targeting Workplace Harassment in Quebec: On Exploring a New Legislative Agenda" (2004) 8 Empl. Rts. & Employ. Pol'y 423.

Perrin, Stephanie *et al. The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Toronto: Irwin Law Inc., 2001).

Picher, Michel G. "Truth, Lies and Videotape: Employee Surveillance at Arbitration" (1998) 6 C.L.E.L.J. 345.

Platt, Priscilla, Lisa Hendlisz & Daphne Intrator. *Privacy Law in the Private Sector: An Annotation of the Legislation in Canada*, looseleaf (Aurora: Canada Law Book, 2002).

Poirier, Marc-Alexandre. "Employer Monitoring of the Corporate E-mail System: How Much Privacy Can Employees Reasonably Expect?" (2002) 60 U.T. Fac. L. Rev. 85.

Polley, John W. "Employment Law Update: NLRB Rules on Employee Use of Company Email for Union Purposes" (2008), online: Faegre & Benson LLP <http://www.faegre.com/articles/article_2391.aspx>.

Posner, Richard A. "The Right of Privacy" (1978) 12 Ga. L. Rev. 393.

Prost, Antoine & Gerard Vincent, eds. *A History of Private Life: Riddles of Identity in Modern Times*, trans by. Arthur Goldhammer (Cambridge: Harvard University Press, 1991).

Radwanski, George. “Workplace Privacy: A New Act, a New Era” (2001-2002) 2 Lab. Arb. Y.B. 1.

Ramasastry, Anita. “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>.

Rasky, Holly L. “Can an Employer Search the Contents of Its Employees’ E-mail?” (1998) 20 Adv. Q. 221.

Richmond, Lorne A. “Employee Use of E-mail and the Internet: A Union Perspective” (2001-2002) 2 Lab. Arb. Y.B. 45.

Rigg, C.L. “The Right to Privacy in Employment: An Arbitrator's Viewpoint” (1991) 1 Lab. Arb. Y.B. 83.

Rosen, Jeffrey. *The Unwanted Gaze: The Destruction of Privacy in America* (New York: Random House, Inc., 2001).

Sack, Jeffrey, Paula Chapman & Juliana Saxberg, eds. “*PIPEDA* Round-up: Privacy Commissioner Examines Use of Employee Medical Information, Workplace Surveillance, and Discipline for Violating Privacy” (July/August 2005) 21 *Human Rights and Workplace Privacy Reporter* 1.

——— *et al.*, eds. “Governments Move to Limit Employees’ Internet Access and E-mail Use” (November/December 2000) 24 *Collective Bargaining Reporter*.

Saint-André, Yves. “Le respect du droit à la vie privée au travail: mythe ou réalité?” in *Développements récents en droit du travail*, Vol. 205 (Cowansville: Les Éditions Yvon Blais Inc., 2004) 51.

Sarra, Janis. “Employee Use of E-mail and the Internet: An Arbitrator's Perspective” (2001-2002) 2 Lab. Arb. Y.B. 11.

Scassa, Teresa *et al. An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies* (28 April 2005), online: Dalhousie University <http://www.library.dal.ca/law/Guides/FacultyPubs/Scassa/RFIDs_Report2(Single).pdf>.

Schafer, Arthur. “Privacy: A Philosophical Overview” in Dale Gibson, ed., *Aspects of Privacy Law: Essays in Honour of John M. Sharp* (Scarborough: Butterworth & Co. (Canada) Ltd., 1980) 1.

Schmitz, Patrick W. “Workplace Surveillance, Privacy Protection, and Efficiency Wages” (2005) 12 Labour Economics 727.

Schoeman, Ferdinand David. *Privacy and Social Freedom* (Cambridge: Cambridge University Press, 1992).

———, ed. *Philosophical Dimensions of Privacy: An Anthology* (Cambridge: Cambridge University Press, 1984).

Schwartz, Paul M. & Joel R. Reidenberg. *Data Privacy Law* (Charlottesville: Michie, 1996).

Selmi, Michael. “Privacy for the Working Class: Public Work and Private Lives” (2006) 66 La. L. Rev. 1035.

Shaffer, Gregory. “Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards” (2000) 25 Yale J. Int’l L. 1.

Sherrard, Michael G. “Workplace Searches and Surveillance versus the Employee's Right to Privacy” (1999) 48 U.N.B.L.J. 283.

Solove, Daniel J. & Marc Rotenberg. *Information Privacy Law* (New York: Aspen Publishers, 2003).

Sookman, Barry B. *Computer, Internet and Electronic Commerce Terms: Judicial, Legislative and Technical Definitions* (Toronto: Thomson Canada Limited, 2007).

Sotto, Lisa J. & Elisabeth M. McCarthy. “An Employer’s Guide to US Workplace Privacy Issues” (2007) 24 The Computer & Internet Lawyer 1.

Spaeth, Juliana M., Mark J. Plotkin & Sandra C. Sheets. “Privacy, Eh!: The Impact of Canada’s *Personal Information Protection and Electronic Documents Act* on Transnational Business” (2002) 4 Vand. J. Ent. L. & Prac. 28.

Stanton, Jeffrey M. & Amanda L. Julian. “The Impact of Electronic Monitoring on Quality and Quantity of Performance” (2002) 18 Computers in Human Behavior 85.

Stephen, Scott P. *Masters and Servants: the Hudson's Bay Company and Its Personnel, 1668-1782* (Ph.D. Thesis, University of Manitoba Faculty of Arts, 2006) [unpublished].

Strandburg, Katherine & Daniela Stan Raicu, eds. *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation* (Chicago: Springer, 2006).

Taggart, Stewart. "Call It the SyDNA Olympics" (7 March 2000), online: Wired <http://www.wired.com/science/discoveries/news/2000/03/34774>.

Taranto, Alicia & Megan Inwood. "Federal Court Now First Stop for Privacy Breaches" (2004) 1 Can. Privacy L. Rev. 129.

Tassé, Roger. "Québec to Challenge the Constitutionality of PIPEDA" (2004) 1 Can. Priv. Law Rev. 49.

Tealby, Jim. "E-mail & Privacy at Work" (1999) 10 J.L. & Info. Sci. 207.

Townsend, Anthony M. & James T. Bennett. "Privacy, Technology, and Conflict: Emerging Issues and Action in Workplace Privacy" (2003) 24 Journal of Labor Research 195.

Turnbull, Ian J. *et al. Privacy in the Workplace: The Employment Perspective* (Toronto: CCH Canadian Limited, 2004).

Uteck, E. Anne. *Electronic Surveillance and Workplace Privacy.* (LL.M. Thesis, Dalhousie University Faculty of Law, 2004) [unpublished].

VanDyk, Evan. "Avatars of the World, Unite!" *Slaw* (1 May 2008), online: Slaw <http://www.slaw.ca/2008/05/01/avatars-of-the-world-unite/>.

———. "Memory" *Slaw* (16 October 2007), online: Slaw <http://www.slaw.ca/2007/10/16/memory/>.

Veilleux, Diane. “Le droit à la vie privée – sa portée face à la surveillance de l’employeur” (2000) 60 R. du B. 1.

Victorian Law Reform Commission. *Workplace Privacy: Final Report* (Melbourne: Victorian Law Reform Commission, 2005).

Wacks, Raymond. *Personal Information: Privacy and the Law* (Oxford: Oxford University Press, 1989).

Wallach, Shelley. “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.

Warren, Samuel D. & Louis D. Brandeis. “The Right to Privacy” (1890) 4 Harv. L. Rev. 193.

“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>.

Watson, Nathan. “The Private Workplace and the Proposed ‘Notice of Electronic Monitoring Act’: Is ‘Notice’ Enough?” (2001) 54 Fed. Comm. L.J. 79.

Weckert, John, ed. *Electronic Monitoring in the Workplace: Controversies and Solutions* (Hershey, PA: Idea Group Pub., 2005).

Wen, H. Joseph & Pamela Gershuny. “Computer-based Monitoring in the American Workplace: Surveillance Technologies and Legal Challenges” (2005) 24 Human Systems Management 165.

Westin, Alan F. “Social and Political Dimensions of Privacy” (2003) 59 Journal of Social Issues 431.

———. “Privacy in the Workplace: How Well Does American Law Reflect American Values?” (1996) 72 Chicago-Kent L. Rev. 271.

———. *Privacy and Freedom* (New York: Atheneum, 1967).

Wheelwright, Karen. “Monitoring Employees’ Email and Internet Use at Work – Balancing the Interests of Employers and Employees” (2002) 13 J.L. & Info. Sci. 70.

White, Jerrod J. “E-Mail@Work.Com: Employer Monitoring of Employee E-Mail” (1997) 48 Ala. L. Rev. 1079.

Willborn, Steven L. “Consenting Employees: Workplace Privacy and the Role of Consent” (2006) 66 La. L. Rev. 975.

Willis, E.B. & W.K. Winkler. *Labour Arbitration: The Year in Review 2006* (Aurora: Canada Law Book, 2007).

———. *Labour Arbitration: The Year in Review 2005* (Aurora: Canada Law Book, 2006).

Wood, Ann Marie. “Omniscient Organizations and Bodily Observations: Electronic Surveillance in the Workplace” (1998) 18 International Journal of Sociology and Social Policy 132.

Woolgar, Steve, ed. *Virtual Society? Technology, Cyberbole, Reality* (Oxford: Oxford University Press, 2002).

Wright, Jeremy. “I Was Just Fired for Blogging” (5 January 2005), online: Ensight.org <www.ensight.org/archives/2005/01/05/i-was-just-fired-for-blogging/>.

York, Andrea & Lisa Carty. “Biometrics in the Workplace: Balancing Technology and Privacy” (2006) 16 E.L.L.R. 21.

——— & Bonny Miller. “Privacy in the Ontario Workplace: A Review of the Draft *Privacy of Personal Information Act, 2002*” (2002) 12 E.L.L.R. 25.

Young, Jason. “The Blogger in the Workplace: Considerations for Employers and Employees” (2005) 6 Internet & E-Commerce Law in Canada 9.

Zweig, David & Jane Webster. “Where is the Line between Benign and Invasive? An Examination of Psychological Barriers to the Acceptance of Awareness Monitoring Systems” (2002) 23 J. Organiz. Behav. 605.