

# **Under the Radar?**

## **The Employer Perspective on Workplace Privacy**

**By Avner Levin, Mary Foster, Mary Jo Nicholson and Tony Hernandez**  
Research assistance provided by Christa Austin and Imran Badshah

## Acknowledgments

This project has been funded through the Contribution Program of the Office of the Federal Privacy Commissioner and through in-kind contributions from the Dean of Business at Ryerson University. The research team wish to thank the project participants who were willing to give up their valuable time in order to advance understanding of the policies and practices associated with workplace privacy. This project would not have been completed in such a timely fashion were it not for our very able research assistants, Christa Austin and Imran Badshah, who worked tirelessly throughout the survey design and data collection phases of the project.

## Introduction

For some time, Canadians have been debating the privacy and protection of personal information, and the merits of different perspectives on this issue. Within the parameters of this debate, Canadians recognize that absolute privacy and individual control over information is neither obtainable nor desirable for a variety of reasons. In addition, the context in which the debate is held, such as health-care, national security, consumer privacy or workplace privacy may have an influence on the strength of views and the perspective that is supported.

On the one hand, Canadians in their role as employees, whether directly or indirectly through organized labour representatives, consistently indicate a strong desire for some minimal measure of privacy or private life in the workplace, as well as an expectation, possibly unfounded, that some degree of workplace privacy already exists. On the other hand, Canadians in their role as employers and consumers recognize the need to balance workplace privacy with other interests to ensure a competitive economy. The purpose of this report is to document current practices in the workplace and to understand how this balance is currently understood and implemented in a Canadian context.

There is some confusion as to whether privacy in the workplace is similar in its scope to the privacy offered by corporations to their customers and business partners with respect to their personal information. Retailers and other corporations in Canada have operated for some time now under the jurisdiction of federal and provincial personal information protection statutes. Great efforts have been invested in corporate compliance with these statutes and to ensure that the personal information provided by an individual to a business in the course of a commercial transaction such as the purchase of goods is protected as required by law. What has flown somewhat under the radar is the comprehension that in certain circumstances the employees of a business are entitled to similar protection with respect to the personal information that the business obtains on them in the course of their employment. This entitlement to workplace privacy originates in federal and provincial legislation, which will be discussed below, and these concepts have become familiar to retailers due to the application to commercial transactions. The conceptual approaches to workplace privacy, are however, based on the nature of the employment relationship itself and are at times quite distinct from the commercial foundations of personal information protection legislation.

There are currently two main conceptual approaches to workplace privacy, which could be broadly termed “a property-focused approach”, and “a rights-based approach”<sup>1</sup>. The *property approach* focuses on the fact that employers own the workplace including the resources that employees may be using for private purposes such as computers and telephones. As a result of this ownership, employers are free to dictate to employees the manner in which such resources are used and employees only have privacy rights, or more accurately expectations of privacy, to the extent that employer policies allow. This is predominately viewed as the US approach to privacy.

The *rights approach* is based on a belief in the dignity and right to private life that is afforded to every human being. Such rights can be balanced against other interests in the workplace, but can never be fully ignored. Employees are entitled therefore to some minimal standard of dignity, privacy and a private life even while working and while using workplace resources, similar to their entitlement to other minimal standards such as minimum wages and days of rest. This position is predominately viewed as the European approach to privacy.

Regardless of the approach adopted, the right of employers to supervise and monitor the performance of their employees has long been recognized in Canada. Traditionally, workplace supervision has been conducted by designated employees, such as managers and supervisors, but also by technological means, such as punch-clocks and detailed telephone bills. The regulation of such forms of supervision is largely decided through the contractual bargaining between employers and employees. Today, however, new technologies present employers with an ability to monitor employees at an unprecedented level. Not only do new technologies exist for the act of monitoring, such as global positioning systems (GPS), but new technologies also exist for the processing of information gathered by monitoring. Employers now have the capability of processing and retaining vast amounts of information produced by their monitoring through key-stroke software, e-mail logs, internet usage archives, Voice Over Internet Protocol (VOIP) digital records, and Radio-Frequency Identification (RFID) tracking systems.

Because the technology at the employer’s disposal is flexible and adaptable, it may lend itself to secondary uses. For example, GPS and RFID are increasingly crucial for supply-chain and product-delivery management. Surveillance cameras are important for inventory control. However, once such systems are introduced into the workplace for

one purpose, the low costs associated with their adaptation for other purposes, such as surveillance to ensure productivity, raise fundamental privacy issues.

The confluence of new means with which information on employees can be collected, with expanding applications by which such information can be processed and retained, is transforming the workplace rapidly. From the employee perspective, there are concerns that a certain measure of privacy and a certain sphere of private life previously taken for granted in the workplace may no longer exist. Collective and individual bargaining may fail to address such concerns in an era where employees in the private sector are increasingly unorganized.

Canadian employers interviewed for this report have another perspective. Privacy is often viewed as simply another 'weapon' in a trade union's bargaining 'arsenal', not as a substantive employee concern. Employers believe with absolute certainty that currently issues involving workplace privacy are appropriately managed. To the extent that workplace privacy is a burgeoning issue, our information suggests that it may be developing under the radar screen of Canadian employers, hence the title of this report. Although employers are aware of workplace privacy in a general sense, there is little in-depth knowledge about whether the dominant approach in Canada is more similar to the European or American approach. They also lack significant knowledge about the extent to which workplace privacy is protected under federal and provincial information protection legislation. This report aims to provide policy makers and employers with insight into common themes and concerns about privacy among Canadian employers, as well as the practices and approaches to workplace privacy currently in place. Ultimately, the aim of this report is to provide information that will contribute to the development of a Canadian perspective on privacy in the workplace that reflects Canadian values and a Canadian context, rather than simply choosing to adopt either the European or the American perspective on this issue.

## The Legal Terrain

Canada is a federation with legislation regulating employment at both the federal and provincial levels, based on the division of powers between the federal level of government and the provinces described in the Constitution. At the present time, workplace privacy, and correspondingly workplace surveillance and monitoring, are not explicitly addressed in the various provincial and federal employment standards and labour relations legislation. As a result, some

employers have arrived at the conclusion that such conduct is the employer's prerogative, based on the traditional, contractual common law approach to the employment relationship. This is interpreted as meaning that the employer retains the prerogative to manage work as the employer sees fit and as long as the employer has not contracted away certain aspects of this prerogative. According to this approach, an employer who enters into a contract with individual workers or with a representative trade union, may assume an obligation to refrain from certain forms of monitoring or surveillance (presumably in exchange for some concession on the part of the workers). Conversely, an employer who has not contracted away any of these rights is unrestrained by legislation in terms of how employees are managed.

Canada has however, in addition, personal information protection legislation at both the federal and provincial levels, that is applicable to the various levels of government, and in some cases to the private sector. In other words, companies and organizations operating in different provinces may have to conform to different provincial rules. As this report focuses on private sector workplace privacy, the (limited) protections offered to public sector workers will not be discussed.

## Federal Legislation

**PIPEDA.** The private sector in Canada is governed by default by federal legislation known as the Personal Information and Electronic Documents Act (PIPEDA), which came into effect with respect to federally regulated employers as of 2001, and with respect to other members of the private sector (although not in their capacity as employers) in 2004. That is, the legislation applies to the private sector across the provinces in the absence of substantially similar provincial legislation. The determination of whether provincial legislation is substantially similar is done by the federal Ministry of Industry Canada, and to date, the provincial legislation of Quebec, British Columbia, and Alberta has been found to be substantially similar (these provinces are further discussed below). Ontario's personal health information protection legislation has been found to be substantially similar for the purposes of health records. Other provinces have so far opted not to pass private sector personal information protection legislation.

**Limits of PIPEDA.** Although PIPEDA has a broad reach in that by default, it covers the private sector across Canada, it only explicitly applies to federally regulated workers

because of the constitutional division of powers. Thus while federally regulated workers in the telecommunication, banking and inter-provincial transportation industries are covered, the vast majority of workers in each province are not protected by PIPEDA. However their employer might be bound by PIPEDA with respect to their customers' personal information. Interestingly, as we discuss later in the report, the awareness created by PIPEDA's application to consumer privacy has trickled into the employment relationship as well. Those workers that are protected by PIPEDA are ensured that their employer must detail the purposes for which their personal information is collected, not collect more information than necessary for those purposes, must keep the information accurate, must notify the workers that the information is collected, although exceptions are allowed in certain circumstances, and must allow the workers access to the information, and the ability to challenge any inaccuracies they perceive in the information collected.

**What is Personal Information?** The immediate question, therefore, is what is 'personal information' for the purposes of PIPEDA and any applicable provincial legislation? Although those we interviewed believe it includes the information about workers that is collected for personnel purposes, such as statutory deductions, the legal definition of personal information is broader. It is defined in PIPEDA as "information about an identifiable individual" although it "does not include the name, title or business address or telephone number of an employee of an organization"<sup>2</sup>. In other words, all the information held by an employer on a worker that can identify that worker, with the exception of the worker's business contact information is personal information and therefore subject to PIPEDA's or the applicable provincial legislation's restrictions. An image captured by a video camera, a personal email sent to a friend, or a telephone conversation with a family member all qualify as personal information.

The restrictions imposed by PIPEDA on the collection, use and disclosure of personal information in the workplace do not mean that workplace surveillance is unlawful. Such a conclusion necessitates an examination of the purposes for which such surveillance is conducted, and PIPEDA is largely silent on the matter. However, PIPEDA does allow the collection of personal information without many of the restrictions mentioned above in particular circumstances, such as for law enforcement purposes, i.e., when a law enforcement agency is involved in surveillance, or for national security purposes, again, when conducted by the relevant agency. A more detailed discussion of some legitimate purposes is found in the next section on provincial legislation.

## Provincial Legislation

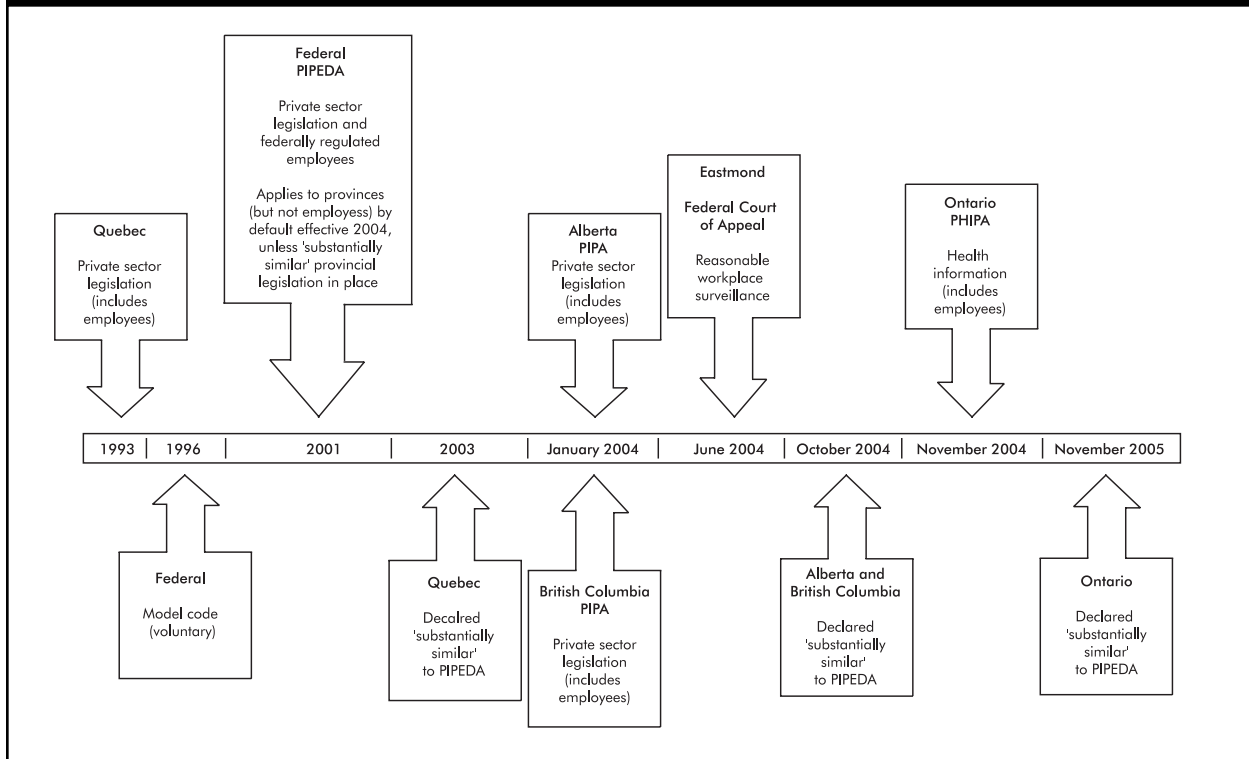
Quebec is the only province to have had private sector personal information protection legislation prior to PIPEDA (see Figure 1). Quebec's private sector personal information legislation, An Act Respecting the Protection of Personal Information in the Private Sector, enacted in 1993, does not include specific provisions with respect to the workplace. As it does not exclude information held by an employer on workers from its definition, it must be read in tandem with Quebec's Civil Code, which obligates employers to respect the dignity of workers<sup>3</sup>. Read together, employers in Quebec are prevented from conducting workplace surveillance for a purpose that, or in a manner that, does not respect their workers' dignity. The implications for specific technologies and purposes will be discussed later in the report.

Alberta's and British Columbia's legislation is similar and both statutes were enacted in 2004 in response to the passage of PIPEDA. Both statutes have a similar name – the Personal Information Protection Act (PIPA). Both statutes deal directly with personal information in the workplace. Employers are permitted to collect, use and disclose personal information for the general purpose of managing the employment relationship as long as the collection, use and disclosure are reasonable. Whereas Quebec requires employers to respect the dignity of their workers, Alberta and British Columbia require only that employers act in a reasonable manner<sup>4</sup>. The distinctions between these two approaches, and the question of which purposes can be considered to fall under the general management of the employment relationship, appear to mirror the differences between the American and European approaches to workplace privacy, and will be discussed later in the report.

## Case Law

It is instructive to examine the existing Canadian case law, i.e., judicial decisions about workplace privacy. Although there are quite a few labour arbitration decisions with respect to workplace privacy, a discussion of these cases is beyond the scope of this report. There is, to date no tort, that is, private legal action, in Canada, for the harm created when one person invades the privacy of another. For this reason, workers must base their legal claims solely on the legislation discussed above. Interestingly, to date there is only one case in which workplace surveillance issues have been examined. However, there are a number of findings from the respective provincial and federal privacy

**FIGURE 1. Privacy Legislation Timeline**



commissioners with respect to workplace surveillance, but space precludes an exhaustive discussion of all these findings. *Eastmond v. Canadian Pacific Railway*, the one case to-date, is based on such a finding. The case involved a railway employee's – a federally regulated worker's – complaint about the installation of video surveillance cameras in the workplace. The complaint appeared to be the result of a disagreement between the worker's union and the railway over the installation of cameras, which led the employer to install cameras unilaterally. Section 5(3) of PIPEDA states that: "an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances". The court endorsed a four-part test, established originally by the Federal Privacy Commissioner in his findings, to determine whether any workplace surveillance is reasonable: "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?" The court then noted that the railway did not intend to monitor workers, but installed the cameras for other purposes including the ability to monitor unauthorized entries and to prevent resulting

theft. The court also found that the fact that the railway's cameras would operate automatically actually serves to reduce the risk of privacy invasion, since it was not at all clear that tapes would ever be reviewed. It was only when individuals reviewed the tapes, ruled the court, that personal information was considered to be collected. The court concluded that the employer was permitted to install the cameras<sup>5</sup>.

In order to determine whether workplace surveillance is reasonable, and therefore legal, the court considered the particular purpose for the surveillance, and determined whether the benefit achieved by the surveillance is proportional to the workers' loss of privacy. It follows that not every purpose, and not every manner in which surveillance technology can be used, would automatically be reasonable. Significantly, the determination of whether workplace surveillance is reasonable is achieved independently of the employer's policies and the notifications issued to workers, which seem to be the aspects most employers focus on when attempting to legitimize their practices, as will be discussed in the report.

# Project Goals and Objectives

The primary goal of this project was to provide a review of workplace privacy practices from the perspective of employers. Since workplace privacy concerns are primarily driven by employees, this project focused on bringing to the fore some of the issues, concerns and interests that motivate employers in their adaptation of new and existing workplace technology, and evaluated the degree to which employers are aware of the privacy-related implications of their surveillance and monitoring measures and activities.

Specifically, this project addressed the following objectives:

- Determining the forms of monitoring/surveillance currently in use or that are planned to be used by employers.
- Identifying and describing the primary business reasons for engaging in monitoring/surveillance from the employer perspective, such as low costs and new technology versatility.
- Inquiring whether there are business reasons for allowing employees private use of employer resources, and whether employers view private use as increasing productivity under certain circumstances.
- Ascertaining the degree of employer awareness of workplace privacy concerns.

- Establishing whether employers perceive that employee privacy is in fact eroded by new measures taken as compared with existing forms of monitoring and surveillance, or whether employers perceive workplace privacy concerns as invalid.
- Identifying the detrimental affects on employers, as they see it, should they face additional obligations to ensure privacy in form of new legislation or regulations, such as an inability to implement valuable technology, loss of productivity or loss of competitiveness in a global economy.
- Determining the degree of interest on employers' behalf in participating in self-regulatory measures such as voluntary guidelines or model codes on workplace privacy, in the spirit of industry cooperation that led to Canada's information privacy protection regime.

## Methodology

### Design

In-depth interviews were conducted with seventeen key informants who have decision-making authority for workplace privacy policies. For logistical reasons, we interviewed two people from one company at different times. An interview with a privacy expert who advised firms about their privacy obligations is excluded from Table 1. The interviews were conducted face-to-face in the office of the interviewee by one or two members of the research team, and

**TABLE 1. Characteristics of Sample**

Number	Sector	Unionized	No. of Employees
1	Hospitality	Yes	Less than 1,000
2	Retail	No	1,000 < 10,000
3	Retail	Yes	Over 10,000
4	Retail	Yes	Over 10,000
5	Retail	Yes	Over 10,000
6	Technology	Yes	1,000 < 10,000
7	Professional	No	1,000 < 10,000
8	Technology	No	Over 10,000
9	Retail	Yes	1,000 < 10,000
10	Professional	No	Over 10,000
11/12	Hospitality	Yes	Less than 1,000
13	Professional	Yes	1,000 < 10,000
14	Retail	No	Over 10,000
15	Technology	Yes	Over 10,000
16	Hospitality	Yes	Over 10,000

**TABLE 2. Characteristics of Refusals**

Sector	No. of Contacts	Unionized	Size (No. of employees)	Reason Given or Issue Identified
<i>Professional</i>	12	None	1 to 150,000	- too small - too busy - not interested - recent bad press about company
<i>Retail</i>	6	Yes: 1 No: 2 No info: 3	1,000 to 150,000	- not interested - recent bad press about company
<i>Hospitality</i>	9	Yes: 2 No: 2 No info: 5	1,000 to 10,000	- too busy - not interested - recent bad press about company
<i>Technology</i>	4	None	1,000 to 150,000	- not interested
<i>Other</i>	3	Yes: 2 No info: 1	1,000 to 10,000	- too busy - not interested

lasted from 60 to 90 minutes. All interviews except one were audio-taped and notes were taken to supplement the tape-recordings.

### Final Sampling Framework

In total, 51 workplace privacy informants were contacted, of which 17 agreed to participate, a positive response rate of 33 percent. As Table 1 describes, we interviewed representatives from 15 companies: 3 in the hospitality sector, 3 in technology, 3 in professional, and 6 in retail (including two companies that had a major presence in manufacturing). Eleven companies had a least some unionized employees, and all but three operated across Canada. For the purposes of confidentiality, all interviewees and their companies are identified by number only, and only the range of employees is indicated.

We recognize that those who agreed to be interviewed may represent innovators with respect to privacy. They felt confident enough in their knowledge to answer questions about the topic and were willing to share the experiences of their firm. Thus, we felt it was equally important to examine the characteristics of those who declined the

opportunity to discuss privacy. Table 2 presents a description of those who refused to conduct an interview, their corporate demographics and the reasons for their refusal.

Interestingly, in only about one third of this group could we readily identify a privacy officer. In addition, the most prevalent reason for not participating is simply non-response to repeated contacts. This suggests that privacy has not emerged as a major issue for many companies in Ontario.

### Instrument

We developed a structured interview schedule based on a thorough review of the workplace privacy literature and the objectives outlined in the previous section. The questions included the following:

1. What is your official title?
2. What are your responsibilities around the issue of privacy? Have they always been part of your job description, or did these responsibilities develop in recent years?

3. From the employer's perspective, what are the main issues that relate to workplace privacy? Have these issues existed in the workplace for a long period or have they developed recently? If recently, what caused them?
4. I would like to ask you about some specific technologies that may be in place in the workplace. Are there currently in place any technologies that could be, or actually are, used for monitoring? Which specifically?
5. What is the primary purpose of these technologies?
6. Are there any secondary purposes? Would you please describe them?
7. Are there any plans for installing any other such technologies in the future?
8. What would be the purposes that these technologies would serve?
9. As far as you know, how do employees feel about these current and intended monitoring systems? Have concerns ever been raised? If yes, in what context?
10. To the best of your knowledge, from your employees' perspective, what are the main issues that relate to workplace privacy?
11. What is the employer's view of the employees' concerns? Are they warranted? What is their motivation? How does the employer plan to address them, if at all?
12. Overall, does the employer perceive that new technologies have had any adverse affect on employee privacy?
13. Are there other privacy concerns, unrelated to technology, that have been voiced by employees? Are they warranted? How does the employer plan to address them, if at all?
14. There is an opinion that all resources in the workplace belong to the employer and therefore that any employee use of resources for private purposes is solely at the employer's discretion. Does your employer agree?
15. At the same time, there is an opinion that some measure of privacy must be granted to employees in the workplace in order to ensure and even increase productivity. Would your employer agree with this opinion? If so, what is this measure? How does your employer ensure this level of privacy?

16. There is an opinion that the current federal privacy legislation created onerous obligations with respect to personnel records. Would your employer agree?

17. Is there an increased burden on the employer in the area of workplace privacy as a result of federal, or other, privacy legislation?

18. If new legislation or regulations were to be enacted that set up additional obligations for employers to ensure employee privacy, such as an inability to implement some forms of technology, what would be the implications? Internally in terms of productivity? Externally in terms of global competitiveness?

19. What is your employer's view of the effectiveness of self-regulatory measures such as voluntary guidelines or model codes as a way of ensuring workplace privacy? Are there other mechanisms that might be effective?

20. Do you collaborate with other employers in your industry or sector on workplace privacy issues?

21. Are there other issues or concerns about workplace privacy that we have not asked you about, and that you would like to comment on?

The interview schedule and recruitment techniques were vetted by the Research Ethics Board of Ryerson University and appropriate consent forms were signed by all those agreeing to be interviewed.

## Analysis

All the interviews except one were transcribed verbatim. One interviewee did not want to be taped and in that instance interview notes were taken. All interviewees were given the opportunity to review either the transcribed interviews or the notes taken during the interview and to ask for corrections to be made. The final transcripts/notes were reviewed by all four members of the research team independently. Two meetings were held to discuss identified themes, issues and trends and to discuss areas where differences in opinion had occurred. The results of that combined analysis are presented in the following sections, according to the stated objectives of the project. In order to protect the confidentiality of our project participants' direct quotes are attributed by number of the corporation as opposed to any personal identifier. The number in brackets after the quote refers to the number of the corporation in Table 1.

## Results

### Employer Awareness of Workplace Privacy

A primary focus of the project has been to establish the level of awareness among employers about workplace privacy, and whether it is an issue that concerns them already or will concern them in the future. Our interview-based data reveal that the reality is that none of the corporations represented by our interviewees identify workplace privacy as an issue of current concern. As one respondent notes, *"I don't think it's even jumped on the radar"* (3). Another suggests that *"workplace privacy is a meaningless term"* (8) because as most employers agree privacy is *"not an issue"* (5) or at most *"a sleeper issue"* (3). One of the anticipated problems before the implementation of the legislation was that employers would be overwhelmed with requests by employees to view their files and that the contents may be the focus of controversy and conflict. According to respondents, employers have not been deluged with privacy requests because *"people [employees] aren't aware"* of privacy as a concern (3), and because workplace privacy as a concept *"hasn't become defined yet"* (4). Most employers report that they *"are not aware of any issues where concerns have been expressed with respect to any of the monitoring that happens"* (7). After the introduction of privacy legislation, there was *"no spike in people requesting to see their files."* (16). The consensus is that *"to this date, we have not received a formal privacy complaint anywhere in the country and a couple of requests for access since the legislation has been in place and that is the extent of it."* (4) In other words, workplace privacy, from the perspective of Canadian employers has been a non-issue to date.

Furthermore, corporate responsibility for workplace privacy rests with different executives and different functional areas depending on the corporation. Contrary to expectations, our interviewees indicate that responsibility for these issues does not always lie within the purview of the human resources department. However, when workplace privacy is identified as a dedicated responsibility, the position is most often housed within the HR department. *"I naturally assumed that I would take it on because I oversee all legislation that affects employees. So I went in there and educated the CEO and executive team that this is coming up. It was just natural"* (6).

Among our interviewees, few report privacy issues as their only area of responsibility. Most report having other responsibilities in addition to privacy, and the privacy-related responsibilities tend to focus more on consumer

issues than on workplace privacy issues. Subsuming privacy concerns under broader employee relations issues or mixing it with other responsibilities is reflected in the corporate titles for those responsible for the privacy portfolio, which include: *"Chief Operating Officer and Chief Privacy Officer"*, *"Director of Labour Relations and Policy"*, *"Privacy and Ethics Officer and Senior Director Employee Development and Services"*, *"Vice-President Human Resources and Privacy Officer"*, *"Chief Privacy Officer and Chief Information Officer"*, *"Vice-President Employee Relations"*, and *"Chief People Officer"*.

Several employers report that privacy in general only became a focus *"after PIPEDA came into place"* (2), although one company has had an employee privacy policy in place for *"between 25 and 30 years"* (14). Interestingly, we found that corporations that recognize workplace privacy as a distinct issue have been aware of it for quite some time – often for at least twenty years. Corporations that deal with workplace privacy as a component of customer privacy developed awareness of both issues only recently, usually when Canadian private sector privacy legislation was implemented. As a result of this legislation, the primary focus of those with responsibility for privacy has been on customer privacy. Any attention to workplace privacy has been somewhat of an afterthought because the main focus of this legislation was on the protection of customer privacy. Nevertheless, employers report believing that they have a clear responsibility *"to make the[employee] file more fact-based than perception-based....In that sense it has added an expense to the company....At the same time, as a company we've always been sensitive to protecting privacy because we have so many customers, we were doing the same thing for our employees"* (15). That same employer went on to point out that because the legislation seems to have been written to address issues in customer privacy, it is not always a good fit for issues of workplace privacy. *"I would say that when PIPEDA was introduced, it was more focused on the customers' side. The employer side was more of an afterthought. They didn't do a good job of connecting it to other pieces of labour legislation. We're caught in that area of other pieces of legislation requiring certain things that infringe on some of the personal information in the privacy legislation."* (15)

Finally, we should note that awareness of workplace privacy as an issue is created not only through legislation and the employment relationship. Consumer personal information protection has garnered a lot of media attention in recent years, and we expect that the media will increasingly turn their attention to workplace privacy issues as well. For example, the tension between the primary and secondary

uses of technology is illustrated in a recent newspaper report: The headline reads “*Montreal to use GPS to keep tabs on workers*”. The story indicates that two Montreal municipalities are installing GPS technologies at a cost of at least \$1,000 per vehicle “*as part of a pilot project to collect data on the comings and goings of city equipment*”. While the municipal politicians suggest that “*the measure is simply aimed at improving the delivery of municipal services*”, the author of the article suggests that the municipalities “*are turning to technology to keep tabs on the city’s notoriously work-shy blue-collar workers*.”<sup>6</sup>

## Forms of Monitoring/Surveillance

Not only were we interested in the general awareness of employers about workplace privacy as an area of concern, but also about their knowledge of the existence and capabilities of a variety of technologies. Employers appear to have a relatively limited awareness of either the technology that is currently in place in their company or its capability. Despite the supposed centralization of privacy concerns in one office, part of this lack of awareness about technology is that some of these systems are under the responsibility of different departments; for example IT is in charge of computer systems, and the logistics area is in charge of GPS and RFID used for distribution and inventory control. As a result, when we asked about specific types of surveillance or monitoring, the reply was more often than not “*I am not sure I can answer that question 100% [about blocked Websites]*” (2).

All employers we interviewed use at least some of the following technologies and practices, which could be viewed as potentially having an impact on privacy:

**Closed Circuit Television (CCTV).** Although all employers use some form of CCTV in the workplace, the technology used for obtaining an image of the workplace varies greatly from one employer to the next. Generally, the more sophisticated the video-technology, the greater the potential impact on privacy, an observation that applies to the other technologies discussed below. The technology continuum ranges from still-cameras that project but do not retain images, through video cameras that retain images on video tapes with limited storage capacity, and are erased periodically as a result, to digital cameras with pan and zoom capabilities and a centralised digital file retention system.

Interestingly, one employer who recently introduced advanced CCTV into the workplace conducted a process

recommended by privacy advocates known as a Privacy Impact Assessment (PIA), in order to assess the impact the new version of the technology would have on the workplace. The PIA was initiated by the employer, even though employees, motivated by safety and security issues, were overwhelmingly in favour of CCTV and did not object to its deployment.

**Access Control System (ACS).** All employers have some version of ACS in place in some sections of the workplace. Typically, ACS is some form of card-swiping technology, with a magnetic strip and usually a photograph, uniquely identifying the employee. This technology facilitates monitoring of staff entering and existing secure areas by time of day and location.

**Digital Point-of-Sale (DPOS).** “*I’m not a ‘techy’ person, but my understanding is that we can track transactions, so we know that at this time of day, this transaction occurred*” (2). This term encompasses a variety of technologies that control point-of-sale devices, such as computerized and networked cash registers. Three employers use some form of DPOS, with the most advanced systems using biometric identifiers.

**Supply Chain Management Technologies.** Two technologies are increasingly being adopted by employers for the primary purpose of supply chain management, both of which may have a potential impact on workplace privacy. The more common one is the Global Positioning System (GPS), introduced by employers into their vehicle fleets. The one less common is the Radio Frequency Identifier (RFID), currently being experimented with by the employers in our study, but not actually implemented. “*Radio frequency has been explored in a very piloted way so far. Again, only in the context of our warehouses for packing purposes, but not right into the stores*” (5).

**Telephone Recordings.** Five of the interviewees represent corporations that operate call centres as part of the workplace, and they all use telephone recordings in their call centres. None of the employers, whether they operate a call centre or not, reports considering the use of this technology in any other area of the workplace. Only one employer has installed a digital telephone system, known as Voice Over Internet Protocol (VOIP). Although VOIP has a significant potential to diminish workplace privacy through the enhanced ability of the system to log and retain telephone conversations, the employer did not consider VOIP to have workplace privacy implications.

**Personal Computer Monitoring.** Several technologies are used to monitor the different ways in which employees use personal computers in the workplace. Many employers retain e-mail messages on central servers. *“All of our e-mails are retained. All our computers are backed up every day, so the content of every hard drive is backed onto a central system”* (7).

Another technology used by our interviewees is the monitoring and logging of websites accessed by employees through personal computers, where such access is available. Indeed, employers limit access to some parts of the Internet both in terms of website content (e.g., pornographic, or gambling websites) and in term of employee rank, which could in itself be viewed as a restriction on workplace privacy. Although roughly half of the employers we interviewed were aware of additional technologies, such as key-stroke monitoring software, and other forms of spyware (software that can be installed on a personal computer to monitor its use) no employer admitted using, or even contemplating using such technologies. On the other hand, it is clear that such technologies are in use in Canada as evidenced recently by an order from Alberta’s Privacy Commissioner which discusses the installation of such software on a library worker’s computer.<sup>7</sup>

**Employee Records.** When presented with a list of technologies and workplace practices that could potentially impact workplace privacy, the interviewees identify personnel records as the main issue related to workplace privacy. This was also the only area in which employers detect a greater level of interest is personnel records on the part of employees. Once employees are made aware that access to their personnel records is available either as a legislative requirement in some provinces or as the result of an across-the-board policy, there have been requests to view files. However, most employers characterize this interest as reflecting curiosity, rather than some deeper concern over privacy.

These records are of concern to employers mainly in terms of the information they contain, and procedures that have been put in place to allow employee access to these records. *“We try to make sure that employee records are maintained and secure, both electronically and on paper. We try to make sure that no information is given out without appropriate consent or given out at all unless absolutely necessary”* (2). All employers have some form of computerized database where personnel records are stored. The information collected varies by each employer, although there are some minimal statutory requirements (e.g., a Social Insurance Number). All employers recognize, particularly with respect to long-

term employees, that some information, for example, marital status and religion, considered relevant to employment at that time, is no longer relevant.

Employers take one of two positions with respect to these records and the information they contain. Those taking one position implement policies and procedures to ascertain the information contained in each record, and then delete unnecessary information. The other position implements policies to ensure employee access to records, and leaves the decision about what irrelevant information is retained in the files within the hands of the individual employee.

According to one employer, some employees are quite happy to continue receiving birthday cards for their children from their employer. *“We didn’t feel the need [to review records] and this is where we are taking a risk. This is where I’m looking at some of business practices and you have to walk the line”* (6). Most employers have not systematically and proactively reviewed their records for the purpose of removing illegal entries. Instead, they give employees access to their own files and remove anything flagged by the employee. *“What we are following is that if the employee requests to have the information removed, we remove it”* (3). *“Given our size and volume, we did not cleanse or look at every file....We would have taken the approach that said the collection of that information was within implied consent for the most part. Anything in a file is there because there was some implicit understanding that you’re giving it to me for the purposes of administering your benefits and payroll....When an individual does request to see their file, their file is reviewed and it’s ensured that anything that’s inappropriate would be removed”* (5).

## The Purposes of Surveillance

Employers identified the following purposes as legitimate purposes for which the technologies listed above were used:

- Safety and Security for workers and customers
- Worker-related theft
- Worker conduct in violation of human rights legislation
- Worker conduct viewed by the employer or co-workers as offensive
- Vehicle fleet maintenance
- Information systems management
- Knowledge management
- Worker training and development
- Productivity

Employers were asked whether some technologies were used for more than one purpose, and if so what that secondary purpose would be. Almost all employers interviewed agree given the purposes listed above, that using technology to measure productivity could be such a secondary purpose. However, all are adamant in claiming that they do not in fact use monitoring and surveillance technologies to measure productivity. *“Everyone has their own way of measuring productivity, but surveillance isn’t one of them”* (1). Call center workers were a notable exception in that their productivity is measured using recorded conversations.

Although none of the respondents reports actively pursuing the secondary capabilities of these technologies, they acknowledge that helpful information is collected through monitoring that can uncover larger business problems. *“For example, I call them cash registers, but really they’re all just computers now, and they’re all centrally connected. If I were the head of security here, I could go in on my computer anytime during the day and look up any transaction that’s happened at any of our stores and at any given time, any one of them. I could call up the receipt of that transaction and show graphically what happened. I don’t need to physically be there to do it. You could call that a monitoring tool. Well we don’t use that technology to monitor the performance of a sales person, in the sense that we don’t record their speed or their proficiency or anything like that, what we do do is produce what we call a report. For example, if a particular cash register in one of our facilities has an unusual number of returns in one day or an unusual number of voids, things that would lead a company to suggest that there’s some fraud going on, maybe some theft, maybe some inappropriate handling of cash, or if there is regular shortages several days in a row on a bigger cash register, then that would lead us to investigate and examine all of the transactions that took place that day and possibly use that data to interrogate somebody about”* (3).

**Purposes of CCTV.** Despite the advanced technological features, all employers perceive the sole purpose of CCTV to be safety and security. *“Our union pushed for the introduction of cameras...they were concerned for the safety and security of their members. Privacy was not an issue... they’re there to protect people and for security purposes”* (2). *“The main purpose of [cameras] is for safety and security”* (11). Most appeared quite unaware of the potential use of CCTV for other purposes, such as productivity, and rejected this use as inappropriate for their workplace. *“Certainly we would never use surveillance to comment generally on somebody’s performance. We don’t measure the number of boxes that somebody lifts in an hour through the*

*use of video camera and rate them on it in their performance reviews”* (4). The only secondary use that employers acknowledge for CCTV was for worker-related theft, although employers insist that such an investigation would be prompted by other indicators initially, with CCTV only used to secure irrefutable evidence of criminal conduct *“the camera tends to provide evidence that can be admissible into a court of law”* (13). *“The main goal of ....monitoring is sort of a combination between loss prevention and safety...What is clear is that we do not employ specific monitoring technologies that are only targeted at employees.”* (4) However, the same employer went on to qualify this statement: *“The only time that a camera would be employed in a hidden perspective would be what we call a last resort in an investigation of an employee theft or fraud situation where there was compelling evidence, but we do not have any physical evidence against them”* (4). In one company, some management staff *“wanted cameras in every stairwell... set up so someone at home could log on and see what was going on. I [Privacy Officer] didn’t want any part of that”* (16).

**Purposes of ACS.** Although ACS may be used potentially for productivity measures, all the employers interviewed report being unaware of this potential use. The purposes identified for using this technology include safety and security, potential liability issues as a result of worker misconduct or offensive behaviour and worker related theft.

**Purposes of DPOS.** Although the technology does have a potential impact on workplace privacy all employers using DPOS view its primary purpose to be inventory control, with a secondary purpose of worker-related theft.

**Purposes of GPS.** None of the employers currently using GPS reports being aware of its potential impact on workplace privacy. *“I don’t know if there has been a need [for GPS] from a monitoring perspective. It’s really more of a locating your truck, where it is, and those types of things”* (3). They view it as a supply chain management tool, and as a fleet maintenance tool, with a secondary application for worker-related misconduct. Interestingly, 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.

**Purposes of Telephone Recordings.** The primary purpose of telephone recording is worker training and development. Although one employer noted that *“What we don’t do is use recorded customer calls as a performance management tool”* (4), three of the employers that operate call centres use the technology by playing back conversations to

employees and pointing out deviations from customer-service training, for the purpose of improving customer service. Improved customer service and increased resolution of customer complaints, is in turn an aspect of productivity for those working in call centres. *“Calls are monitored...as a measure of productivity”* (3). And another employer stated: *“I’ve seen it in a couple of situations where we’ve monitored the minutes on certain calls when persons have put themselves on hold, where they are calling when they are on hold, and how long they are on hold, as opposed to dealing with customers. We’ve used that and we’re about to use that”* (15).

**Purposes of Personal Computer Monitoring.** The primary purpose for which e-mails are retained is driven by technology – information systems management. The central server system is seen as a back-up repository on which employees at times simply store their messages, and from which e-mails may be retrieved in the event that they are never received by the intended party, deleted inadvertently, or lost by some form of computer system malfunction. None of the interviewees reports conducting routine analysis on e-mails. *“The only analysis that I’m aware of with respect to e-mails is just the traffic volumes”* (7). However, employers do retain e-mails for secondary purposes including potential liability issues stemming from employee misconduct, such as defamation, intellectual property infringement claims, breach of contract or confidence and insider trading claims, as well as law enforcement requirements, and as a safeguard against potential external or internal complaints about employee conduct that might be deemed offensive (e.g., pornographic e-mails, racist e-mails and so on). No employer uses or contemplates the use of these retained e-mails for productivity purposes, although the technology is available to analyse e-mail messages according to the addresses to which they are sent, content keywords and so on. *“We did monitor e-mail several years ago. We didn’t find it was an objective use of time...if you are a good manager you’re asking your employees the right questions to ensure they are engaged, you should know”* (6). Not only does this type of monitoring not represent a good cost-benefit investment, but for many employers it seems to conflict with their preferred workplace environment. *“We did make a conscious decision when we moved into this building to not introduce systems and processes that were going to monitor our computer usage and web usage, on a “big brother”, watching you all the time way. That was kind of our general approach in terms of how much time is worth spending doing all of that for catching 1% of offenders”* (5).

Employers view both website logging and curtailed access as necessary for both the resource management of informa-

tion systems and out of fear of employee misconduct that might result in either criminal conduct or create civil liability for the employer. *“We like to be reasonable about it, so I think reasonable is what we go by. As far as blocking sites, we do have a bandwidth issue in the first place, and we spent a lot of money in updating our platforms, so we are always worried about bandwidth and what this is going to be used for. It shouldn’t be at the expense of our customers. So we do block sites. We block gambling and inappropriate sites because we feel that this is not the way to use bandwidth”* (10). Employers would be willing to *“go into those logs, if there was a problem and an employee was being investigated for a certain reason”* (9).

Although all employers are particularly aware of the potential abuse of personal computers by employees for personal browsing, and the resulting productivity loss, no employer admits to the use of Internet monitoring technology for productivity measuring purposes. Employers were also clear that productivity cannot be measured in keystrokes. Productivity is viewed as more complex than the amount of time spent on the computer or the length of telephone calls. Employers felt that those choosing to measure productivity this way were missing the point. In addition, managers would be well aware of unproductive employees through good supervision, and the additional information provided by a report on keystrokes or internet time would only reinforce what was already known through conventional good management practices. *“I’ve heard people measure keystrokes. We don’t do any of that kind of stuff”* (2). *“Basically, if there’s any kind of a performance issue or an employee seems to be falling down on a job, that’s why they have a manager or a supervisor to be able to catch that and discuss it with them before they have to do any radical monitoring of behaviour”* (9).

## The Justification for Privacy in the Workplace

The justification provided by employers for workplace privacy was based on the conceptual basis of privacy that they affiliated themselves with, as broadly put to employers in the interview instrument under Questions 14 and 15. These questions sought opinions about the viability of both the American, property-based approach to the workplace, and the European, human rights, dignity-based approach. The answers of employers to these questions seem to indicate to us a certain degree of tension between the approach which employers are often told to adopt, by internal and external legal counsel and other consultants – the property-based approach, and the approach to which employers tend to gravitate out of their own practices and

workplace culture. This approach is not exactly based on full fledged recognition of an employee inalienable right to dignity as is the case in most European Member States either. Instead, it appears to be a unique Canadian approach, based on the value of trust. *"We've always operated ...in a trust environment. We trust people. We believe they trust us. As some point or another, behaviours are questionable. We don't need a camera to address the situation.....That doesn't mean that some people are not dishonest, [but, we do not want to create] an environment where people feel they are spied on"* (11). *"I don't know that we actually need....legislation of any kind to know that we want our information to be kept confidential. I think it's more of a common sense, it didn't need to be legislated to exist... what I think is that pre-legislation, there was a stronger element of trust. We trust our employees to keep it confidential and the employer would actually see it the same way. But we want to treat others the way we want to be treated"* (10). Another employer suggests that *"it was always part of [the] job description to link good morale and trust in the workplace and the company connected the two. [The employer] connected employees' right to privacy"* (1), with the overall corporate culture that was founded on principles of trust. Other employers comment on the tension between the property-based approach and the workplace culture: *"I would think our philosophy would be when push comes to shove, I think [the property-based approach is] too extreme. Once again, you really want your employees when they're here to feel part of a larger organization. Part of feeling engaged is feeling you belong. If you were constantly reminded that's our desk, that's our computer, that would contradict our main goal, which is to feel like they belong, that they are part of our organization. But at the end of the day, the policies do state, we have a right when you go checking illegal websites...but we are not constantly shoving these policies down their throats"* (6). The importance of employer-employee trust was highlighted by another employer. *"Basically, we say that the interest of the company and the interest of the individual are inseparable and so it is important to protect employee data to run the business while maintaining the privacy of individual personal data. We feel strongly about building that foundation of trust between the employee and the company"* (14).

**Policies.** Notwithstanding this strong viewpoint of trust as the cornerstone of the employment relationship, the practical justification for workplace privacy, as it is found in employer policies and practices, is based on the stated claim of all employers: *"[Workplace resources] are private property and only persons authorized by the owner may access [them]"* (9). Some employers do not have any policies or standard practices in place with respect to their use of these tech-

nologies. They refer to their current practices as 'common-sensical', 'reasonable' or 'obvious' and therefore as not requiring any particular policy as part of the employment relationship. *"If you want to get really technical, employees have no privacy rights currently. No enshrined privacy rights. Basically, when it comes down to the [legislation] there is a section ...that actually excludes all employment related records. So technically speaking, we can do everything and anything that we want to. But from an HR perspective and a common sense approach, it does not make sense to take that approach because you're only going to be cheesing people off and upsetting them"* (9). Those employers with a generic policy in place typically emphasize that workplace resources are private property, and therefore that these resources can be used by the employee solely at the employer's discretion. The policy then lists just some of the purposes mentioned above as examples (most frequently the policy would identify human rights legislation and potential worker criminal or offensive conduct). The technologies in use went unmentioned.

Neither did most employers have in place a policy or executive guidelines as to how requests for personal information were handled internally. Based on the interviews, it appears that IT departments use their discretion with respect to such requests that typically came from managers or supervisors of individual workers. Often it would seem that the HR department simply relied on the good sense of the IT workers who had access to the information by virtue of the information system structure, so that control of the manner in which personal information was used was haphazard at best. *"With computers you've got the IT area, you've got the legal, you've got the policy folk, you've got the privacy folk. You're talking about having one universal approach and I say the more people you ask, the more opinions you're going to get"* (9). The common explanation put forward by employers for this state of affairs was that it reflects the low priority of workplace privacy for both the employer and the employee, or more specifically that workplace privacy is a 'non-issue' in terms of the employment relationship, as previously discussed.

Some policies concerning technologies with potential privacy issues are enacted as a result of employee requests rather than any proactive planning on the part of employers. For example, workers often ask for particular technologies, such as video surveillance or access control, out of pressing concerns for their personal safety and security. Despite framing the use of technology as part of their overall concern for employees, there continues to be a perception on the part of employers that it is their prerogative to conduct monitoring

and surveillance by almost any means necessary. For example, when asked for an explanation about why productivity is almost never measured employers indicate that technology is simply not the best tool with which to measure productivity. No employer offers as an explanation that such use of technology will insult their workers or affront their dignity. Indeed, all employers agree, when asked directly, that the workplace is the employer's property and thus has the right to conduct surveillance. No employer agrees with the proposition that workers are entitled to some measure of privacy that cannot be taken away. Employers rationalize the measures of privacy that exist within their workplace (e.g., the lack of cameras in their washrooms) as necessary in order to retain and attract desirable workers, and as beneficial and conducive to productivity, but not as the manifestation of some worker legal or human right.

Most employers report having adopted or being in the process of adopting policies that relate to the technologies described earlier. *"In the coming months we are going to be implementing [our employee] privacy policy"* (5). These policies reflect the purposes identified by the employers for the technologies and at times have little to do therefore with workplace privacy. Those employers that do not have, or do not plan to have such policies take the view that use of these technologies is subject to "common-sensical" rules that do not need to be spelled out. *"This firm employs extremely sophisticated people... Our people are not naïve... We don't stand up and tell that [they are monitored] to them. They've learned that before they joined us. We assume our people have a reasonable degree of sophistication and they know that there's a record"* (7). Further on this legal perspective is concern about exposure to liability. *"I think that privacy is growing as a concern in any type of policy that you develop, and as Commission decisions are becoming increasingly stringent and various tribunals about this. Just as any other case law has developed, employers become more and more concerned about how new policies, procedures, techniques are going to increase exposure for them to be the victim of litigation or media scrutiny"* (4).

With respect to those technologies that could serve a secondary law-enforcement or employee misconduct purpose (such as CCTV and personal computer monitoring) those employers that do have a policy or are in the process of implementing a policy mention these purposes as being the motivation for the policy. In addition, they describe the procedures involved in implementing the technology for these secondary purposes including level of authorization required and the courses of action open to employees suspected of misconduct. *"They all know there is*

*a policy regarding sites, jokes and that kind of stuff that is enforced. The system blocks if there is certain wording: the system will block it"* (11).

Employers believe they have created awareness of privacy issues among employees in a number of ways. For instance, CCTV policies have been brought to the attention of employees through signs posted in conspicuous locations. As employers acknowledge, these signs serve the additional purpose of alerting the public. Half of employers with computer monitoring policies in place have informed employees through a notice that comes up on the employee's computer screen every time the computer is turned on, and which employees must accept in order to use the computer. *"Every time you turn on your computer, a notice comes up...that says [you] understand the rules under which this [computer] is to be used"* (2). The other employers require employees to sign off on the policy annually, or at the time of hiring. *"Every new hire is given [the code of conduct] and they have to sign it as a condition of employment"* (5). *"When they first join the firm, they go through an introduction process where they are exposed to policies and procedures and they have to sign off that they understand them and they will comply with them. There are some annual sign-offs along the same line to reinforce and refresh it"* (7) *"We have them sign a yearly 'accountability' paper. It already exists, but we just added in a clause that contains privacy..."* (3). Still other policies, for other technologies, such as the employee record management system, are circulated or made available to employees via other resources such as a workplace Intranet, but in these instances there is no sign-off requirement.

**Practices.** All employers agree with the proposition that some form of workplace privacy, which employers call "personal space" or "private life", is necessary for the regular and trouble-free functioning of their corporation. *"Privacy is one of our core values, a crucial element of good business sense and a building block for [our] success"* (1). This is often discussed in the context of "respect" and "trust" as mentioned above. Some employers are even sympathetic to the notion that an increase in workplace privacy, which they view as a privilege granted to employees, may result in an increase in productivity, although the form of increase expected varies from one employer to the next. In fact, one company *"encourages its employees to use these technologies [employer-provided Internet, e-mail and telephone] for their own purposes. [It] has policies on [its] site that actually says that"* (15). In another instance, the employer finds it quite acceptable to allow employees to conduct on-line personal banking transactions during work, while another does not. *"We don't have a policy of no personal calls or e-mails, because*

*sometimes it's actually better for productivity if someone can send a quick one minute e-mail to somebody that's important, rather than have to take a break and then go somewhere else for ten minutes to do the same thing. So we just say that people are expected to be reasonable. They are expected to do their job, but we're not going to be unreasonable and say that they cannot have a life when they are here. Just like you have personal things in your desk, you have personal phone calls and e-mails, but they must be reasonable. That is our philosophy"* (10).

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. *"We know people use the Internet for personal use. We look at it as a management responsibility. We're not inclined to monitor people's activity or do this through surveillance.....Everybody knows what they are supposed to be doing and they know whether or not they're being productive....If people use the Internet or e-mails for personal things on occasion, we're reasonably lenient. As long as it's not violating any of the areas of where you're not supposed to go and it's not interfering with productivity"* (2). *"We don't work with machines; we work with human beings...We have to remain flexible for employees in order to be realistic in our expectations"* (11). Despite this reported flexibility with respect to the personal use of employer resources, employers do indicate they will be lenient *"as long as there isn't rampant abuse."* (9) However, if an employee *"steps over the boundary and it gets to be an abusive situation, when [he/she] is misusing work property or corporate property, then....there is a problem."* (9)

**Costs.** Further justification for allowing or tolerating private use of employer resources is based on the perception that the costs of installing and utilizing surveillance technology are simply too high. Most employers feel that if they were to analyze data, reportedly collected for mostly safety and security reasons, from a productivity perspective it would be a waste of resources with few benefits delivered. *"It's all the information in all your systems that you have about my comings and goings which could be cameras, could be clocks, could be physical access cards, because those for the most part are digital. Would we have a challenge pulling that all together comprehensively and exhaustively? Absolutely. We would not be able to do that very well"* (5).

Employers also point out the tremendous financial resources that will be necessary for keeping such technology up-to-date and making sure that the same systems and capabilities

are widely available. In this respect surveillance technology is more of a resource issue for employers than it is a workplace privacy issue. *"Some people, I think sometimes fail to recognize particularly with the use of technologies around surveillance is that there's actually a huge financial burden associated with monitoring technologies....We would probably react negatively to a law that said you have to put this type of camera in every corner of your building..You're going to pay for the technology that is going to manage your inventory....that's spending to improve efficiencies rather than to act as some kind of deterrent or somehow catch more people"* (4).

## The Role of Government

Employers were asked about their perception of both the past and future role of government in workplace privacy. Depending on their range of operations, employers were asked about the role of the federal and the relevant provincial governments, as well as the relevant privacy commissioner. In an emerging area of importance, such as workplace privacy, government has a potential future role through future legislation, regulation and suggested guidelines. What became apparent as a result of the interviews is that employers perceive government as having played a significant role, through the introduction of legislation and through the offices of the various privacy commissioners, in the creation of awareness to privacy and the protection of personal information in general. The educational role associated with simply introducing the legislation cannot be underestimated.

**Past Role.** The development of legislation related to privacy motivated our respondents to take formal steps to comply with the requirements. The majority of employers in our sample turned their attention to the development of a (general) privacy policy after 2001 after PIPEDA had passed but before it applied to the provincial private sectors. Three employers report that their general privacy policy was only fully developed in 2004 when PIPEDA came into force over those provinces that lacked substantially similar legislation. With the exception of those employers who clearly fall under PIPEDA's mandate as federally regulated employers, and therefore have policies and practices in place even prior to 2001, PIPEDA was an eye-opener to employers as it created awareness, where little existed before, about the personal information they held on customers and its impact on their customers' privacy. It appears that only now, several years later, are employers becoming aware that the information they collect on employees through monitoring and surveillance could be thought of, under PIPEDA, as personal information as

well. In addition, employers that operate under provincial legislation in BC, Alberta or Quebec appear more aware of workplace privacy than employers operating in other provinces (primarily Ontario in our sample). These differences underline the educating and awareness-increasing role that the provincial legislation has played.

**Future Role.** We did not expect any employer to advocate a greater role for government in the arena of workplace privacy and our expectations have been largely fulfilled. *"I don't think you will find anyone who will tell you that they need more government interference in their business"* (4). *"Well I'm fine with clarification [of the legislation], but in terms of extension, I would think the business community would be more in terms of saying let us digest what we've got, before you start piling on more"* (7). Employers have different reactions to the several possible roles for government in the area of workplace privacy. No employer sees any need for additional federal legislation on privacy in general, and on workplace privacy specifically. This, again, is as expected. Half of our interviewees whose companies operate nationally, but are not federally regulated, are the most concerned about this possibility, although they report being willing to consider as the 'lesser evil' the possibility of federal legislation that would not deviate from, or increase the standards of, the relevant provincial privacy legislation with which these employers already have to comply (BC, Alberta and Quebec). In fact, 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.

All of the employers we interviewed were subject in some form to PIPEDA, although as mentioned above not necessarily for their workplace privacy practices. However, having gone through the implementation process of PIPEDA in the years preceding 2004, all employers report being negatively disposed to the prospects of going through a similar process should the reach of PIPEDA be expanded to workplace privacy issues for non-federally regulated industries, or should additional workplace privacy legislation be introduced. Employers were content with the legislation remaining as is, providing them with principles of personal information protection without unduly restricting the process by which such principles were to be attained. *"I think Canada has done well at this point...building a piece of legislation that is principle-based and leaves the decision makers enough room to take the individual situations which are always incredibly complex and unique and allow you to apply them with reason. You go down the path of making things more black and white and you run into*

*problems where you can no longer properly interpret. Then, the whole exercise becomes more rules-based and proving and disproving as opposed to getting back to the spirit and principle of what we're trying to do.... protect people's personal information and the use of it"* (5). *"I'm very uncomfortable with trying to find black and white answers because there is only a context and that's what happens in setting precedents. Precedents look at what happened in the context of how and when it happened. So I think to try and find black and white answers is going to be very difficult"* (10). All employers expressed dismay at any notion of linking contractual relationships with the federal government to any form of workplace privacy compliance or audit program, that might be similar for example, to the obligations imposed on federal contractors in the area of employment equity.

The Federal Privacy Commissioner cannot legislate of course, but is free to offer guidelines and best-practices solutions to workplace privacy issues (e.g., guidelines for the use of CCTV), which employers are then able to adopt should they choose to do so. When asked about such voluntary guidelines, four employers express some interest in such guidelines. Within these, all of the employers with unionized workforces see guidelines as actually beneficial, since the existence of guidelines enables them to defuse any potential workplace privacy issue and remove it from the bargaining table or grievance process by simply complying with the guidelines. The majority of employers, however, see no need for additional guidelines on workplace privacy, although they welcome any guidelines that would clarify the already existing legislation.

**Labour Jurisdiction.** Employers with a unionized workplace express concern (that has been echoed for example by BC's Privacy Commissioner) that workplace privacy is currently subject to the jurisdiction of the applicable privacy commissioner as well as to the jurisdiction of labour arbitrators. A potential role for government exists in clarifying the jurisdictional boundaries between arbitrators and commissioners in this area. Some employers feel that workplace privacy is being raised by unions as a "burr under the saddle", in instances where an already somewhat acrimonious relationship exists. *"I think [unions] look at privacy....as one additional way of annoying the employer. A lot of times the questions or complaints I'll get....are not even related to true privacy issues"* (15). Others are not willing to concede their prerogative to manage the workplace, and do not require unionized employees to sign their privacy code of conduct *"because we don't want to get into any conversation with the union that would give any indication or feeling that they could somehow bargain [on this issue]"* (5). On the

other hand, however, some employers enjoy a more cordial relationship with their unions, which is reflected in the area of workplace privacy. *"We would not roll out any technology without consultation... safety is the issue we are hearing from our union"* (13). According to these employers their employees raise no concerns about existing or potential workplace technologies in terms of their privacy implications. On the contrary, employers report that employees advocated the adoption of better technologies for safety and security in the workplace.

Probably the most unexpected finding of this project is the uniform insistence of employers that their employees do not actually have any 'real' concerns related to their privacy in the workplace. *"We are unionized but privacy has never been raised, to the best of my knowledge, as an issue, even in disciplinary proceedings"* (3). We found that regardless of industry, governing legislation, or the degree of organization of the workforce, employers claim that their employees do not perceive workplace privacy as a 'real' issue. Employers note that in the rare instances in which workplace privacy are raised by employees, it has been within the context of some other problem with the employment relationship, such as a ongoing disciplinary process, arguments over promotion, and so on. From the employer's perspective, workplace privacy concerns voiced by an employee are never the main problem in the employment relationship and hence the need to clearly demarcate the jurisdictional boundaries between privacy commissioners and labour arbitrators.

We should note that employers perceive their treatment of all employees, whether unionized or not, and regardless of other distinctions (e.g., probationary/full time) as equal. Professional firms, despite the ambiguity as to the legal status of workers such as partners or consultants are equally committed to the uniform application of workplace privacy policies. *"Partners are held to a much stricter code of content than the junior staff are. That comes with the territory. It's a condition to becoming a partner in the firm is that you're prepared to comply with those high standards. There are differences. But basically people are given a choice, you can agree to comply with them or not during the partnership"* (7).

## The Role of Industry

**Voluntary Codes.** When employers advocate for a lesser role for government in their affairs they usually complement their call with promises that industry can step in and fill the regulatory gap with self-regulatory measures, to the extent that such a gap exists. One recent privacy-related

example, although ultimately unsuccessful in its attempt to stave off legislation, has been the adoption by the Canadian Marketing Association of a voluntary do-not-contact service. Interestingly, the origins of PIPEDA itself are in the Model Code adopted by the Canadian Standards Association. Perhaps somewhat surprisingly, therefore, there was no similar promise of involvement put forward by the employers in our study. *"I think we have all been left to come up with our own policies"* (10).

No employer reports awareness of any work done on common workplace privacy measures within their industry or through their umbrella organizations that usually advocate on their collective behalf (e.g., the Retail Council of Canada). This lack of action on the workplace privacy front was explained quite simply by employers to be the direct result of workplace privacy being perceived as a 'non-issue', to the extent that workplace privacy received any attention at all.

About half of the employers report engaging in a limited form of collaboration including, exchanging policies with other employers in their industry, supplying policies to other employers as templates, or learning from their colleagues' experience. To the extent that we were able to determine, these exchanges, although significant, are the result of personal connections that have developed between executives in similar roles (e.g., corporate privacy officers) rather than a strategic decision made at a higher executive level.

**Voluntary Compliance.** Employers in our study were often faced with the opposite problem – not a lack of legislation, but an abundance of legislative standards. Employers then had to decide whether to simply comply with the distinct demands of each jurisdiction, at an added cost reflecting the complexity of such compliance, or whether to adopt the higher standard with the benefit of simplicity, but the expense of unnecessary compliance in some jurisdictions. Several employers face this problem within Canada, when operating in provinces with and without workplace privacy legislation (such as Alberta and Ontario) and other employers face this problem since they operate outside Canada as well – in the US, Asia and the EU.

When faced with such jurisdictional differences we found that employers opt for compliance with the most stringent legislation. *"We went to the highest standards"* (3). *"We were not interested in having different approaches in different regions. We made the decision that we would rise to the high water mark in all areas, not just in the employee area"* (5).

Employers usually position this strategy in the context of their desire to be the best at everything they do, including conformity with privacy legislation, despite the significant costs. *“I think one of the biggest challenges for companies like ours is the whole national versus provincial framework, having to work with separate legislation”* (5). *“One of the reasons this [Ontario] privacy policy was developed last year was because of the situations that occurred in BC and Alberta”* (3).

**Multinationals.** Canadian employers that are part of a multinational corporation perceive their obligation to be compliance with the relevant Canadian legislation. These employers perceive themselves as caught between a rock and a hard place when their Canadian obligations conflict with their obligations under other jurisdictions, or when their Canadian practices conflict with requirements under foreign legislation. For example, one employer expresses concern about monitoring and surveillance activity in Canada because *“surveillance of employees is absolutely [not done] in Europe”* (14).

Most employers are preoccupied with the legislative requirements imposed by the US, and sometimes they have to commit substantial resources not to protecting information, but to collecting it to meet the requirements of another jurisdiction. *“We have an American parent, which means there are PATRIOT Act issues, going back and forth in terms of how information is managed...Just getting together that information about our practices was probably the most monumental task...”* (4). This external cross-border control of Canadian business practices was felt also *“because [corporations] list [their] stock on the US market, [and they] are subject to legislation that is implemented in the US”* (15). Coupled with the influence of the US is what is perceived as *“the trend worldwide...toward increased surveillance and increased security”* (13). Employers perceive that compliance with US legislation, such as the USA PATRIOT Act or the Sarbanes-Oxley Act, brings about changes to their positions on safety, security, monitoring, surveillance and background checks – in other words, that it creates an atmosphere of distrust of their employees – that has not traditionally been part of the Canadian corporate culture. *“I do think that a certain part of the good governance model is a cultural one. I do think that our history has been a Canadian company and a Canadian environment and what’s considered a Canadian standard of workplace privacy, workplace respect. Those types of things are true in terms of how much self-restraint there’s been in terms of wanting to increase monitoring and increase the amount of information that we collect. I think that is accurate. What we’re seeing in*

*terms of legislation coming down, in my mind, more of a protection of what already been the case in Canada from an outside influence from the United States rather than some type of change in the past. I think what you see is negative influences, particularly from the south, that may want us to increase security all the time, at the expense of other things. What you’re seeing is a cultural response that by saying we can no longer assume that Canadian businesses always behave in these types of ways whether it be in privacy or in corporate governance from an accounting perspective or whether it would be in terms of investment practices and things like that. You can no longer trust that Canadian companies are going to not behave that way, so you need to include legislation that’s going to protect that culture”* (4).

Despite these pressures, the multinationals in our sample feel that they have managed these influences by setting up *“a global standard”* (14) for privacy, that is at the highest level. *“When you are in India, and there are no data protection laws in India, that wouldn’t matter to us because the data that we might be processing in India has to comply with [our company’s] laws and requirements, which are equivalent to the European Union”* (14). As a result, *“[they] have rarely had any issues coming from an area that they are worried about employee privacy”* (14).

**Outsourcing.** Whether multinational or local, employers are coming to the recognition that some key functions with respect to the processing of their employee information are no longer controlled in-house. The third party can be located in the same or in another jurisdiction. As a result, there is increased awareness about the outsourcing of customer personal information, and once again, just as the introduction of personal information legislation created awareness among employers to the privacy of their customers and subsequently their employees, concerns over the outsourcing of personal information in general appears to be driving the protection of the personal information of employees as well.

For example, when some client services are delivered on the employer’s behalf by a third party, it is more difficult to define and to enforce workplace privacy standards because there is a question of whose policies should cover the third party’s employees. With large influential employers, the strategy has been to “enforce” their standards for customer and workplace privacy on the outside suppliers. *“If we enter into agreements with third party companies, we try to make sure that we have signed agreements with them as to how any personal information will be protected, upheld and just basically what PIPEDA says, collection and disclosure”* (2).

This becomes further complicated when those third parties are outside the country. *“We deal with companies [that outsource information outside Canada] and I think we would want to protect our employee information from transferring out of the country. [These corporations] could on occasion transfer the information out of the country. We haven’t been faced with anything like that [but] we know a lot of companies have been faced with American situations”* (15).

## Discussion

It should be said that those employers that operate in a Canadian jurisdiction that lack private sector personal information legislation, such as Ontario, appear indeed to be able to legally exercise their prerogative to conduct workplace surveillance as they see fit. Although, to the extent that these employers operate in other jurisdictions, and to the extent that they have established across-the-board personal information policies or entered into contracts with workers, they could voluntarily place limits on this prerogative. Similarly, it is not unreasonable to speculate that were such an employer to engage in outrageous privacy invading measures, such as washroom monitoring, such a case could lead to the establishment of a common law tort of invasion of privacy in Canada.

Be that as it may, it is certainly not controversial that workplace surveillance for purposes that are legally required is in itself legal. This point is quite distinct from a separate discussion that could and indeed should take place as to what these legally required purposes are in a free and democratic society, and to what extent must the private sector comply with the objectives of the state in which it operates. This is a debate resembling a current debate as to whether Internet Service Providers (ISPs) should be required to hand over the personal information of their customers to the government, and if so, when. It is clear that employers must comply with various applicable statutes, such as collect, use and disclose employee personal information that is used to deduct taxes, pensions or employment insurance. Employers must also comply with law enforcement or national security agencies in their investigations and exceptions to such effect are incorporated into the personal information protection legislation that exists in Canada.

What is less clear is the extent to which employers are free to initiate workplace surveillance for their own purposes. Considering the list of purposes for which technology may be used to manage some part of the employer’s operations, such as the employer’s vehicle fleet, or their information system, many uses are again relatively uncontroversial.

They seem reasonable, and related to the management of the workplace, to mimic both PIPEDA and the language found in BC’s and Alberta’s PIPA, and provided the technology is not used for any additional purpose they seem to respect the dignity of workers as well, which is the Quebec legislative requirement. Furthermore, they appear to answer the four-point test established in the Eastmond case mentioned previously in that they are necessary, effective and not privacy invasive, provided again that the technology is not used for any secondary purposes.

The bone of contention, if at all, seems to lie with technologies that are used for secondary purposes, or with technologies that are explicitly used for the primary purpose of measuring productivity. To a large extent the contention is a tempest in a teapot, as employers claim not to be engaged in such practices. The employers that we interviewed, however, represent the ‘best practices’ segment of employers with respect to workplace privacy. Even these innovators are not fully aware of the capabilities of current technologies. Given that they continue to claim the prerogative to engage in surveillance, the discussion whether such use is desired, let alone legal, is invaluable.

## Workplace Privacy and Dignity

By far the easier question to answer is whether surveillance via some technology for productivity purposes respects the dignity of workers. There is a large body of European legislation, and some EU case law, to answer this question negatively. The human right to dignity has been largely developed in Europe over the years. It manifests itself as an aspect of privacy as the right of individuals to a private life. The right of all individuals to a private life is protected under Article 8 of the European Convention on Human Rights, and is incorporated into the present draft of the European Constitution. Article 8, and the EU Data Protection Directive, have been incorporated into the legislation of the various EU Member States many of whom already have had such protection.

Read together Article 8 and the Directive, as well as the guidelines put forward by the various EU data protection authorities, impose a regime according to which personal information must be collected, used and disclosed in a manner that respects an individual’s private life. Significantly, the right of an individual to a private life has been recognized by the EU courts to exist in an employment relationship context as well, just as the more general right to dignity continues to exist, and manifests itself in other areas of the employment relationship through health

and safety or minimal employment standards. The right to a private life has led for example the French Supreme Court to decide that employers are not allowed to read employee private e-mail or other correspondence, even if the e-mail has been sent using employer resources, and even if the act of using employer resources for private purposes has been in violation of an employer policy. In other Member States, such as Italy and Germany, employers are forbidden by legislation to introduce any surveillance technologies into the workplace for productivity purposes without the explicit agreement of the representatives of the workers, be they works councils, that is joint worker-employer committees, or trade unions.

The European conclusion is that surveillance by technological means for productivity purposes is generally in violation of the workers' right to a private life. Europe offers employers other alternatives – conduct surveillance for productivity purposes the 'old-fashioned' and more expensive way – using the observations of other workers such as supervisors, or introduce technologies into the workplace in full consultation and agreement with workers and their representatives.

Consequently, should a dispute over such workplace surveillance in Canada ever proceed to trial, and should the court adopt an approach that recognizes the right of workers to dignity and to a private life, it is probable that the surveillance would be ruled unlawful. That is the conclusion that a simple application of the right of workers to a private life would entail, considering the manner in which workplace surveillance is carried out according to employers interviewed for this project.

## Is Workplace Privacy Reasonable?

Luckily for employers the courts in Canada have yet to adopt, fully or partially, an approach to workplace surveillance based on the dignity of the monitored workers, although as mentioned the legislative ground is laid out in Quebec for such an approach. The examination of whether workplace surveillance for productivity purposes is permissible under current legislation and case law must take therefore another perspective into account, and ask whether such surveillance is reasonable.

The requirement that privacy invasive measures be reasonable is set out in PIPEDA's and BC's and Alberta's PIPA, and has been reaffirmed in the Eastmond case, all discussed above. But just exactly how does the court, or the employer for that matter, determine whether a particular technology,

used in a particular way, and for a particular purpose, is reasonable? There are several differing answers to this question. To begin with, workplace surveillance that answers the four-point test established in Eastmond would be reasonable. To some extent, however, this answer merely shifts the focus onto the questions asked in the Eastmond test, and so another perspective on this question is required. Such a perspective may be found in the US approach to issues of workplace surveillance which seems to be largely mirrored in the perceptions of employers we interviewed for this project.

In the US, the determination of whether a particular form of surveillance is reasonable depends in fact upon whether the worker had reasonable expectations of privacy to begin with. US jurisprudence shifts therefore the burden of reasonableness from the employer to the worker. Thus, in the US employers are not asked to justify that their practices are reasonable, as could be assumed to be the case so far under Canadian legislation, but rather workers are asked to justify that their expectations of privacy are reasonable. The former presumes some measure of pre-existing workplace privacy, but whether or not it is based on dignity or some other human right is another question. The latter presumes a prerogative of the employer to manage the workplace as the employer sees fit.

In order to understand what is meant in the US by the phrase 'reasonable expectations' it is necessary to delve to some degree into the legal protection of privacy, such as it is, in the US. American citizens are legally protected from surveillance conducted by their government, primarily through the Fourth Amendment to the US Constitution, which permits only 'reasonable' searches and seizures. In the leading case on the Fourth Amendment the US Supreme Court found that the reasonable expectation of privacy that citizens have is built from the subjective expectations that citizens have, and by that is meant what a particular individual actually believed, and from the objective expectations of US society as a whole, that is common values. Both expectations are necessary in order to construct the reasonable expectations that would govern a particular situation or form of surveillance. In other words, a person that does not have subjective expectations within a given situation as to their privacy, for example, because they have been simply told that they are under observation, cannot claim that they had any reasonable expectations of privacy as well.

This approach has been incorporated from constitutional law into court decisions in US tort law. Since tort law is the

only avenue workers in most of the US have to pursue claims that their workplace privacy has been violated, through a tort known as Intrusion Upon Seclusion, the result is that in the US workers must prove that they have had subjective expectations as to their workplace privacy in order to be successful in their legal action. US employers have therefore been actively attempting to shape and change such expectations by managerial tools at their disposal, such as policies with respect to worker use of workplace resources, for example a policy that would prohibit any use of the email system for personal reasons and notices, for example, a sign that would be posted declaring that a certain area in the workplace is under camera surveillance.

These have proven to be effective legal tools and have made it difficult for workers to protect their workplace privacy as courts have repeatedly found that they had no reasonable expectations of privacy to begin with since they had no subjective expectations of privacy by virtue of a workplace policy or notice. In fact, in one particularly infamous case the courts found that workers had no reasonable expectation of privacy despite a policy that did provide them with some guarantee of privacy in their personal communications, since the policy was found by the court not to apply to the particular circumstances in which the communication was sent. Another outcome of this state of affairs has been a noticeable lack of a discussion as to what, if at all, are the values shared by US society that would constitute the objective portion of the reasonable expectations of privacy under US law.

The legal state of affairs in the US, and the phrases incorporated into some Canadian legislation, therefore, have led Canadian employers to believe, on the advice most likely of in-house or external counsel that, as long as they eliminate through measures such as policies, notices, or contractual provisions any subjective expectations that their workers might have with respect to privacy, they would be legally within their rights to conduct surveillance as they see fit. Hence, we see the widespread adoption of supplementary measures by many employers that require their workers to click their acceptance of pop-up notices at the beginning of the work day on their computers, or to sign off regularly on policies that reiterate the employer's ownership of workplace resources and the employer's prerogative to use these resources as the employer finds fit. Whether that is indeed the case in Canada remains to be seen. It is not at all clear, based on the legislation and the existing case law, that Canadian courts will end up adopting the US approach to determining reasonableness of workplace surveillance –

which is at the end of the day the only legal basis upon which surveillance for productivity purposes can be found lawful.

## Conclusion

The question may therefore well be asked: Is the US notion of 'reasonable expectations' in and of itself reasonable? Does it make sense, or does it lead to absurd results, and will it therefore be adopted in Canada? It seems that any construction of workplace privacy founded on the US notion of reasonable expectations would be founded on quicksand. The American doctrine, thanks to its reliance on the subjective expectations of workers, is a doctrine that knows no bounds. In principle, the US understanding of workplace privacy would permit any form of monitoring and surveillance (e.g., in washrooms, lockers and the like) so long as the workers have been duly notified and have therefore had their individual expectations of privacy eliminated. It is clear that this approach to workplace privacy is lacking some version of minimal standard of privacy that could be potentially found in the US formulation of socially shared objective values that lead to reasonable expectations. Unfortunately, the US is not yet at a stage where US courts will be able to dispense with the notion of subjective expectations as one building block of workplace privacy, and that stage may never appear as long as the US approach is one that is based on tort law, since subjective expectations are a necessary element of almost any tort that incorporates a standard of reasonableness.

Where does this US state of affairs leave Canadian employers? The answer that this report gives is that although Canadian legislation permits reasonable intrusions on privacy, these intrusions cannot be determined as reasonable by referring exclusively to the subjective expectations of workers. In part, this is due to the available course of action for workers being based on legislation, rather than tort law. The interpretation of legislation is not bound by the principles of tort law, and as seen in the Eastmond case discussed above, an independent test for reasonableness has been developed in Canadian law.

Furthermore, although Canadian employers may be influenced by US policies and practices the Canadian privacy authorities are very much aware of the European approach to privacy protection as well. BC's Privacy Commissioner, when discussing the requirement under PIPA, that privacy invasive measures be reasonable, has been explicit: "...in considering the question of reasonableness, it's appropriate, in my view, to balance the dignity interest of employees

with the business interests of employers.”<sup>8</sup> Such a perspective on workplace privacy should indicate to Canadian employers that the determination of whether any particular monitoring or surveillance technology that they adopt is lawful, will not rely solely on the policies and practices that they have put into place. True, in some Canadian jurisdictions there is currently no private sector privacy legislation and no private course of action available to workers, and therefore no barriers to prevent employers from implementing privacy invasive measures as their prerogative. But for many Canadian employers, and in particular the large Canadian employers that are either subject to federal legislation or operate in more than one province and are therefore subject at least partially to provincial private sector privacy protection legislation, the conclusion is not so simple.

While some purposes of monitoring and surveillance are acknowledged and permitted, the invasion of workplace privacy for other purposes, and in particular for the purpose of measuring productivity, may not be lawful. Such use of technology must be reasonable, and in Canada invasion of workplace privacy is reasonable not only if workers had no expectations of privacy as is the case in the US, but only if the right of these workers to their private life and their dignity was sufficiently protected as well. Canada appears to be therefore in the process of developing an approach to workplace privacy that combines the US rhetoric of reasonable privacy protection with the EU substance of balancing monitoring and surveillance with the human right of workers to dignity.

Do workers share the perspective of their employers? Do workers view the employment relationship in Canada as built on trust? Is the relationship of trust the reason why workplace privacy exists as an issue under the radar of employers? Is workplace privacy under the radar of employees as well? And is the expectation of employees to privacy in the workplace based on the trust that exists between them and their employer? This report has inquired into the employer’s perspective on the developing Canadian approach to workplace privacy. Additional research is required into the awareness of employees of their privacy in the workplace, their sensitivities, concerns and expectations, in order to further substantiate the conclusion of this report that a unique Canadian approach to workplace privacy is indeed developing.

## References

<sup>1</sup> For a discussion of the two approaches see Avner Levin & Mary Jo Nicholson, “*Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*”, 2 *University of Ottawa Law and Technology Journal* 357 (2005); Lawrence Rothstein, “*Privacy or Dignity: Electronic Monitoring in the Workplace*” 19 *New York Journal of International and Comparative Law* 379 (2000).

<sup>2</sup> PIPEDA, § 2 (1).

<sup>3</sup> Quebec Civil Code, § 2087.

<sup>4</sup> PIPA §§ 15, 18, 21. (Alberta); PIPA §§ 13,16,19 (BC).

<sup>5</sup> 2004 FC 852.

<sup>6</sup> The Toronto Star, April 26th, pp.A1,A8.

<sup>7</sup> Order F2005-03.

<sup>8</sup> David Loukidelis, “*Arbitrators & Privacy Commissioners: Why They Should Listen to Each Other*”, Insight Conference “*Privacy Laws & Effective Workplace Investigations*”, Calgary, May 4-5, 2004, pp. 6-7.