Workplace Monitoring and Surveillance

Christopher McHardy
Tina Giesbrecht
Peter Brady

March 11, 2005

Hands on support.

Introduction[1]

In the last decade, new technologies in the workplace have changed the way we do work and the way we manage employees. Beyond the production and cost benefits, these technologies have both increased employer risks relating to employee misconduct and improved employer tools to manage and address such misconduct.

The increased risks and improved tools have resulted in increased use of surveillance and monitoring and an increase in the tension between management rights and employee privacy. The introduction of privacy legislation in Canada has further increased this tension. This paper looks at the way in which new privacy legislation is influencing the way courts and arbitrators are balancing the right of employers to know and manage versus privacy rights employees may have in the workplace.

A New Era

Since the implementation of the federal *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*")[2] in January 2001, issues of privacy and protection of personal information have become a regular concern for human resources managers. *PIPEDA* now applies to all commercial activity in Canada except in those provinces which have substantially similar legislation and where the federal government has registered an exemption order. Personal information which flows across provincial or national borders will be subject to *PIPEDA* and *PIPEDA* will continue to apply, within provinces, to the activities of federal works, undertakings and businesses such as broadcasting, telecommunications, banking and transportation.

Alberta's *Personal Information Protection Act* ("Alberta *PIPA*")[3] and British Columbia's *Personal Information Protection Act* ("B.C. *PIPA*")[4] have been in force since January 1, 2004. Both provinces and Quebec, which enacted private sector privacy legislation in 1994, will be exempted from the application of Part 1 of *PIPEDA* in respect of the collection, use and disclosure of personal information in respect of organizations which are not federal works, undertakings or businesses.

These statutes have brought additional considerations to bear on the question of workplace surveillance and monitoring and the traditional arbitral analysis regarding conflicting employer monitoring and employee privacy rights.

Reasons for Monitoring and Surveillance

Employee or Customer Safety

Increasingly, attacks, robberies, violence, workplace mishaps, other workplace safety issues, and associated liabilities and damages provide motivation for employers to monitor the workplace. Remote worker monitoring systems are being used to monitor employees working alone or in isolation by using simple telephone and/or wireless technology with a standard computer workstation. Such systems can identify emergencies and guide response teams through a step-by-step emergency response. Deterrence, responsiveness and enhancing the ability to investigate are common objectives for use of monitoring measures.

---

[1] This paper was prepared by Christopher McHardy and adapted, in part, from "New Privacy Legislation in the Workplace: Issues of Surveillance and Monitoring" authored by Nancy A. Trott and Rosalie A. Cress.

[2] S.C. 2000, c. 5.

[3] Alberta *Personal Information Protection Act*, S.A. 2003, c. P-6.5.

[4] British Columbia *Personal Information Protection Act*, S.B.C. 2003, c.63.

Confidentiality and Trade Secret Concerns

Safeguarding confidential information is another major motivation for using monitoring technology. And, when you look at some statistics, it becomes clear why:

- 80 percent of IT-related crimes are committed from within an organization.[5]
- In 2002, 80 percent of primarily large corporations and government agencies acknowledged suffering financial losses due to computer breaches, with the most serious being losses due to theft of proprietary information, where the largest 26 losses averaged $170,827 million each.[6]
- The average financial loss from computer security breaches in 2002 was more than $2.5 million per company. The most serious financial losses occurred through theft of proprietary information.[7]

Recently, CIBC sued nine former executives and the brokerage they defected to, Genuity Capital Markets, accusing them of a "conspiracy" to solicit colleagues from the bank and taking confidential information with them. CIBC submitted numerous BlackBerry e-mails and PIN messages as evidence that confidential information was taken from the bank and solicitation of employees occurred while the executives were still employed by the bank.

Workplace Liability and Investigations

Potential legal liability resulting from employee computer misuse or misconduct is often a motive for employee monitoring. Incidents of harassment, safety and theft may trigger an investigation into such misconduct that may use monitoring or surveillance.

Racial and sexual harassment claims arising from racist or pornographic Web browsing or e-mails is not an uncommon occurrence. One law journal paper cited the following high-profile cases. Morgan Stanley, the Wall Street brokerage, was sued for US$70 million by employees because of racist jokes that were distributed on its e-mail system and allegedly created a hostile work environment. Chevron Corporation settled a $2.2 million lawsuit with employees who took offense to an e-mail about, "25 Reasons Why Beer is Better Than Women." Xerox Corporation dismissed 40 employees for sending or storing pornographic e-mail or looking at inappropriate web sites - some for up to eight hours a day - during working hours. The New York Times dismissed 22 people at a pension office in Virginia, for passing around potentially offensive e-mails, including some that allegedly included sex jokes and pornographic images. Dow Chemical Company dismissed 50 employees and disciplined 200 others for abuse of e-mail at one of its Michigan plants, which included off-color jokes, pictures of naked women, depiction of sex acts and violent images. Months later, Dow dismissed 24 workers and disciplined an additional 235 employees for the same misconduct at one of its Texas plants.[8]

In 2001, Ontario's Ministry of Natural Resources disciplined 66 employees, six of whom were dismissed for viewing, transmitting and storing pornography and other objectionable material. In 2003, the Yukon Government's investigation into the same kind of misconduct implicated 542 employees and resulted in disciplinary action against 96 people.

---

[5] Russ Cummings. Venture-capital IT firm 3i director. New Media Age Magazine, January 2002.
[6] 2003 Computer Security Institute/FBI Computer Crime & Security Survey: located at http://www.security.fsu.edu/docs/FBI2003.pdf
[7] Ibid.
[8] Elizabeth Cameron and Dawn Swink. "Employee Use Of The Internet: Where Voyage Is Forbidden." The ALSB Journal of Employment and Labor Law. (Fall 2004, Vol. 10, Issue 1).

Network and Systems Performance

Network performance is an important issue for businesses as a downed system can cost hours in lost productivity across the workforce, loss customers and revenue, and untold damage to reputation. Efficiency of the computer network is also an important factor in business productivity and performance. A major concern for employers is network bandwidth traffic, including slowdowns related to employees downloading, sharing and using large audio and video files, Internet surfing and high volumes of personal e-mail. These activities can also introduce viruses that may attack and disable a network.

Employee Productivity

As companies invest heavily in sophisticated PDAs, computers and software for employees, concerns over employee use of employer computer resources is a major motivation for employee monitoring. In 2000, the Angus Reid Group reported that Canadian employees spent about 800 million work hours each year on personal Internet use.[9] The survey found that Canadian employees with Internet access at work averaged eight hours online per week, of which at least two hours were for personal reasons.

Another survey claimed that 25 percent of employees admitted spending 10 to 30 minutes each workday surfing non-related work sites. A further 22 percent admitted spending 30 to 60 minutes each workday surfing non-related work sites. Astonishingly, 12 percent admitted spending one to two hours and 13 percent admitted spending more than two hours each workday surfing Internet sites unrelated to their jobs.[10]

Each of the above concerns can form a legitimate basis to monitor employees. Weighed against these concerns, however, are the privacy rights an employee may have.

The Employer's Right to Know

Courts and adjudicators have recognized that employers have a legitimate interest in monitoring the workplace. Whether for productivity or for security reasons, an employer can protect its economic interests by monitoring aspects of the work environment. Employers may also undertake monitoring to protect themselves from potential legal liability. However, while the employer's right to know what is going on in the workplace has been established, courts and administrative tribunals have placed limits on this right.

The Employee's Right to Privacy

Employees have a limited right to privacy in the workplace. This right finds its origin in a variety of sources, including collective agreements, provincial or federal statutory provisions, the common law and the Canadian Charter of Rights and Freedoms. Courts have provided different interpretations of the limitations on the scope of this privacy right depending on the type of surveillance used by the employer and the circumstances surrounding the surveillance, including the grounds upon which the employer decides to implement surveillance and the reasonable expectations of the employees in each case.

Is There an Expectation of Privacy?

Privacy is increasingly recognized as an important value in our society. The introduction of federal and provincial privacy legislation has changed the way many organizations do business and has generated heightened concerns

[9] "Surveillance Technology: Monitoring Canadians At Work." Innovate Magazine (Spring 2004), located at: http://www.innovationlaw.org/pages/innovate_spring04.pdf

[10] Hans H. Chen, "Internet Use Survey 2000 - Trends and Surprises in Workplace Web Use" Vault.com (September 1, 2000), located at: http://vault.com

about the collection, use and disclosure of personal information. The issue is whether, and to what degree employees are entitled to privacy in the workplace.

The starting point is that if an employer has expressly advised employees that any documents created, sent or received on its computer network are not treated as private and may be monitored or reviewed by the employer, then employees have no reasonable expectation of privacy. As a result, the employer may monitor usage and open or retrieve employee files regardless of whether they are "personal" or work-related.

In the absence of such an express rule, the general legal assumption is that if the electronic network is provided for business purposes, there is no reasonable expectation that an employee's usage of the electronic network is "private", so that the employer may monitor or review usage. This assumption is based on the following factors:

- the computer equipment is the property of the employer;
- it is provided for business purposes;
- documents, including e-mail, are stored through a network main frame which is not private but is accessible by other employees; and
- monitoring or review does not involve any intrusion on the employee or his or her personal effects.

It has been recognized that

> … there is not the same reasonable expectation for personal privacy for those employees who use the … [employer's] e-mail system as there would be by those employees who communicate through a private letter mail system or those employees who engage in a private telephone conversation.[11]

However, this assumption of a lower privacy expectation is not universally held by all arbitrators and courts. Some arbitrators and judges are prepared to accept a modicum of entitlement to privacy, particularly in those situations in which the employer has permitted personal use of its technology or does not have a reasonable basis for monitoring the employee. Furthermore, the principles enshrined in recent privacy legislation have reinforced privacy expectations and protections for employees.

The Privacy Legislation Principles of Consent and Reasonableness

The principle of consent is a relatively unique feature of personal information protection legislation and one that most clearly distinguishes it from earlier jurisprudence.

Except for limited exceptions, personal information about an individual may not be collected, used or disclosed without the knowledge and consent of the individual. Consent must be "informed," meaning that an organization must, on or before collecting personal information, identify the purposes for which the information will be used and disclosed. Prior to obtaining the consent, the organization must disclose contact information for a person within the organization who can answer questions about the collection.[12] In B.C., the name, position and title of the contact person need only be provided on request.[13] Consent may be obtained orally or in writing and may be implied (including by way of "opt-out" consent) in some circumstances, depending upon the sensitivity of the

[11] *Re Insurance Corporation of British Columbia* (unreported., Weiler, January 27, 1994) at pp. 49-50).
[12] Alberta *PIPA*, s. 13(1); B.C. *PIPA*, s. 10(1).
[13] B.C. *PIPA*, s. 10.

information. Where information is particularly sensitive, such as medical or financial information, express consent for the collection, use and disclosure of that information may be required.[14]

The Alberta *PIPA* and the B.C. *PIPA* specifically addressed the unique issues posed by the employment relationship. "Employee personal information" in B.C. and "personal employee information" in Alberta are distinguished from "personal information" generally. In B.C., "employee personal information" is defined as personal information about an individual that is collected, used or disclosed solely for purposes which are reasonably required to establish, manage or terminate the employment relationship between the organization and the individual, including a volunteer relationship[15]. In Alberta, "personal employee information" means personal information reasonably required by an organization that is collected, used or disclosed solely for the purposes of establishing, managing or terminating an employment relationship or volunteer work relationship[16]. Both Acts emphasize that "employee personal information" and "personal employee information" do not include personal information that is not about an individual's employment[17] or is unrelated to that relationship[18].

An employer may collect, use and disclose employee personal information without the consent of the employee as long as it is reasonable for the purpose of establishing, managing or terminating an employment relationship. However, before an organization collects, uses or discloses employee personal information without consent, the organization must:

(a) notify the employee that it will be collecting, using and disclosing the information; and

(b) identify the purposes for which the information will be collected, used and disclosed.[19]

In July, 2004, the Office of the Information and Privacy Commissioner for British Columbia ("OIPCBC"), David Loukidelis, sought public input on his office's development of employment privacy guidelines.[20] The OIPCBC circulated a draft discussion paper entitled "Employment Privacy Discussion Paper and Guidelines" ("OIPCBC Discussion Paper"). On the subject of surveillance and monitoring, the OIPCBC Discussion Paper proposes that notification must state the type of system employed and the locations at which monitoring devices are operative and the degree of surveillance or monitoring which is occurring. It also proposes that notification should state the purposes for collecting the information; the circumstances under which the information will be used and disclosed and the type of employee activity being monitored (for example, employee location). It further proposes that notification of the surveillance should be brought to the attention of employees on a regular basis and notification should be repeated each time the monitoring policy changes or there is a change to policies regarding the behaviour being monitored.[21]

One general exception to the consent requirement which is particularly relevant to the issues of surveillance and monitoring is the "investigation exception", which provides that personal information may be collected used or disclosed without consent if it is reasonable for an investigation.[22] In British Columbia, it must also be reasonable to expect that the accuracy or availability of the information or the investigation itself would be compromised if

---

[14] Alberta *PIPA*, s. 8(3); B.C. *PIPA*, s. 8(3).
[15] B.C. *PIPA*, s. 1.
[16] Alberta *PIPA*, s. 1.
[17] B.C. *PIPA*, s. 1.
[18] Alberta *PIPA*, s. 1.
[19] Alberta *PIPA*, s. 15(3), s. 18(3) and s. 21(3); B.C. *PIPA*, s. 13(3), s. 16(3) and s. 19(3).
[20] "Employment Privacy Discussion Paper and Guidelines" (June 2004), online, Office of the Information and Privacy Commissioner for British Columbia, located at: http://www.oipc.bc.ca/pdfs/private/PIPAEmploymentGuidelines.pdf ["OIPCBC Discussion Paper"].
[21] "OIPCBC Discussion Paper" at 2.2.
[22] Alberta *PIPA*, s. 14(d), s. 17(d) and s. 20(m); B.C. *PIPA*, s. 12(1)(c), s. 15(1)(c) and s. 18(1)(c).

the individual knew of the surveillance.[23] Both Acts contain a specific definition of "investigation" which includes an investigation related to a breach of an agreement.[24]

A key principle under the Alberta *PIPA* and the B.C. *PIPA* is that of reasonableness. Personal information may be collected or used by organizations only for purposes that a reasonable person would consider appropriate in the circumstances.[25] Regardless of whether consent is necessary or has been obtained, the collection, use or disclosure of personal information is prohibited unless it is reasonable.

The legislation seeks to balance competing rights and interests. The reasonable privacy interests of individuals and employees must be balanced against the reasonable needs of organizations to collect, use and disclose personal information in the course of their operations.

In achieving a reasonable balance, there are two key considerations:

(a) Is the purpose reasonable?

(b) Is the scope of the collection, use or disclosure reasonable?

By using the word "reasonable" and referring to the "reasonable person", the legislation invites interpretation by the application of previous jurisprudence. When considering how workplace surveillance and monitoring will be examined under the Alberta *PIPA* and the B.C. *PIPA*, direction may be taken from the judicial and arbitral jurisprudence and findings under *PIPEDA* .

PIPEDA features an "appropriate purposes" provision that limits collection, use, and disclosure of personal information only for purposes that a reasonable person would consider are appropriate under the circumstances" (s. 5(3)). This reasonableness provision limits workplace surveillance since employee consent to surveillance will no longer be sufficient on its own to justify unlimited surveillance activities. This means that general e-mail monitoring, predicated on nurturing a harassment free workplace could be considered a contravention of PIPEDA if there is no evidence showing a need to address the issue.

PIPEDA requires that each subject organization have a privacy officer position, which means employers will have to include such persons in their monitoring and surveillance plans and where access to employee personal information may be needed to address workplace issues.

PIPEDA also has provisions concerning notification of employees regarding workplace monitoring. It requires the employer to identify the purpose of monitoring (Schedule I, Principle 4.2), to obtain consent (Principle 4.3), and to limit collection of personal information to that which is necessary for the purposes identified (Principle 4.4). This effectively creates an obligation to inform employees and limits what may be collected. An exception, however, does give an employer the right to conduct reasonable monitoring without notice if it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province (s. 7(1)(b). This wording imports "reasonableness" with respect to collection of personal information without consent; in other words monitoring can only occur where it is reasonable to assume that knowledge would compromise the accuracy of the information. Also, the collection or monitoring must be reasonable for purposes related to an investigation. Therefore, reasonable surveillance measures can be used which will limit monitoring if there exists an equally or more effective means that is less privacy-intrusive.

[23] B.C. *PIPA*, s. 12(1)(c), s. 15(1)(c) and s. 18(1)(c).
[24] Alberta *PIPA*, s. 1(f); B.C. *PIPA*, s. 1.
[25] Alberta *PIPA*, s. 11 and s. 16; B.C. *PIPA*, s. 11 and s. 14.

Reasonableness is likely to be the key issue in determining the scope and legitimacy of workplace video surveillance under the Alberta *PIPA* and B.C. *PIPA*. The analysis of "reasonableness" will likely follow the contextual balancing set out in recent decisions of the Federal Court of Canada, the federal Privacy Commissioner and labour arbitrators which consider the purpose and scope of surveillance and the privacy rights of employees. While the purpose and scope of surveillance are always important considerations in determining "reasonableness", different considerations will apply depending on whether the surveillance is known to employees or surreptitious. The threshold for surreptitious surveillance will be higher than the threshold for non-surreptitious surveillance.

Disclosed, Non-Surreptitious Surveillance

Four common factors have been considered by arbitrators and the federal Privacy Commissioner in the analysis of what is reasonable video surveillance:

1. Is the surveillance necessary for a legitimate or reasonable business interest? Legitimate business interests often include loss prevention, and safety or security risks.

2. Is the information collected only that necessary to achieve the intended purpose? The scope of surveillance will be reasonable only if it is restricted to what is necessary for achieving the expressed purpose.

3. To what extent is employee privacy affected? Surveillance in areas of productivity or where employees have a reasonable expectation of privacy is usually held to be unreasonable, unless there is a serious, significant business interest at stake. Where employees have a low expectation of privacy, such as at entrance/exit areas, video surveillance may be reasonable for less pressing business purposes.

4. Were alternatives considered and will they be effective? Video surveillance is seen as a significant step or "last resort". If there are other less privacy-intrusive ways of effectively achieving the same purpose, then it may be unreasonable to use video surveillance instead of those alternatives. However, an organization may not be required to use inefficient or costly alternatives, where all the other requirements of reasonableness and necessity are met.

These factors were considered by the Federal Court of Canada in its June 11, 2004 decision in *Eastmond v. Canadian Pacific Railway*.[26] The application before the Federal Court was based on facts which were the subject of a complaint to the federal Privacy Commissioner.[27] Canadian Pacific Railway installed six digital video surveillance cameras at various locations in its Toronto railyard for the purpose of reducing vandalism and theft and minimizing threats to staff safety. The cameras were fixed, did not zoom and only recorded 48-hour periods. Employees were informed of the existence of the system, its purposes and camera locations. Productivity was not monitored and shields were installed or the camera position changed if cameras were inadvertently trained on working areas.

The Federal Privacy Commissioner, in his findings, applied a four-part test to determine the reasonableness of the video cameras in the circumstances. He asked:

1. Is the measure demonstrably necessary to meet a specific need?

2. Is it likely to be effective in meeting that need?

3. Is the loss of privacy proportional to the benefits gained?

---

[26] *Eastmond v. Canadian Pacific Railway* 2004 FC 852 ["*Eastmond*"].

[27] *PIPED Act* Case Summary #114: "Employee object to company's use of digital video surveillance cameras" (Radwanski, Privacy Commissioner, January 23, 2003). Online: Office of the Privacy Commissioner of Canada, http://privcom.gc.ca/cf-dc/2003/cf-dc_030123_e.asp. (last modified.31 March 2004) ["Case Summary #114"].

4. Is there a less privacy-intrusive way of achieving the same end?[28]

The Privacy Commissioner found that, while there was a *potential* problem, the railway had provided insufficient proof that a real and specific need existed to reduce vandalism, theft and improve the safety of employees.[29] The Commissioner was not convinced that the cameras were a deterrent and speculated that signs warning of surveillance alone may have deterred would-be vandals. The Commissioner found that the benefit was not proportional to the loss of privacy felt by employees and was concerned that the mere presence of cameras had given rise to the perception among employees of "being watched".[30] Finally, he held that there were less privacy-intrusive ways of effectively reducing vandalism that were not sufficiently explored, such as better lighting.[31]

The Federal Court disagreed. Noting that all parties had urged the adoption of the Privacy Commissioner's four-part test, the Court stated that it was "prepared to take into account and be guided by those factors".[32] The Court went on to say that *PIPEDA* mandates a balancing of interests, by naming the competing interests at stake in the purpose clause of *PIPEDA*.[33] The Court stated that "the factors which the Privacy Commissioner took into account in this case may not necessarily be relevant in other contexts".[34]

The Court in *Eastmond* suggested that the "four-part test" is not a stringent test for the appropriateness of surveillance but instead lists important factors to be considered in balancing competing interests. The reasonableness of surveillance must be determined contextually, looking at the why, how, when and where collection takes place.[35] The Court reviewed previous arbitral jurisprudence on workplace surveillance and emphasized a contextual and reasonable balancing of interests as the "test", not a list of required elements.

The reasonableness of the video surveillance was evaluated using the four factors and the Court found that:

1. Canadian Pacific proved that there was a clear history of vandalism, theft and other minor crimes in the railyard. Preventing it in the future was held to be a reasonable purpose under *PIPEDA*.[36]

2. The Court found, on a balance of probabilities, that surveillance was effective at preventing vandalism, theft and security risks. It did not agree that signs warning of the surveillance alone might have been an effective deterrent, stating that "warning signs and cameras go hand in hand — you cannot have one without the other."[37]

3. The loss of privacy was held to be low and proportional to the benefit gained by Canadian Pacific.[38] The images recorded were viewed only upon a reported incident. Information was kept secure and viewed only by the manager or the Canadian Pacific police. The images were recorded in "public places" where the individuals had a low expectation of privacy.

---

[28] *Eastmond* at para. 13.
[29] Case Summary #114.
[30] *Eastmond* at para. 14.
[31] *Eastmond* at para. 14.
[32] *Eastmond* at para. 127.
[33] *Eastmond* at para. 129. Section 3 of *PIPEDA* states: "The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances".
[34] *Eastmond* at para. 130.
[35] *Eastmond* at para. 131.
[36] *Eastmond* at paras. 177, 178.
[37] *Eastmond* at para. 179.
[38] *Eastmond* at paras. 180, 181.

4. Canadian Pacific considered alternatives and demonstrated that, given its extensive operations over a wide area, fencing and security guards were not cost-effective and would be disruptive.[39]

On balance, Canadian Pacific's use of video surveillance in the workplace was reasonable: its purpose was appropriate and the use of the camera fit reasonably within that purpose.

The Federal Court's analysis in *Eastmond* is similar to that in arbitral decisions on video surveillance in the workplace. Prior to the enactment of personal information protection legislation, arbitrators generally considered a number of factors in balancing employees' right to privacy and employers' right to protect its business interests.

Arbitral Jurisprudence

The arbitral jurisprudence has generally considered three questions in determining whether the surveillance is reasonable in all the circumstances:

1. Was it reasonable, in all the circumstances, to request surveillance?

2. Was the surveillance conducted in a reasonable manner?

3. Were there equally effective alternatives to surveillance?[40]

In *Unisource Canada Inc. v. C.E.P. Local 433*[41], the employer had installed nine cameras in the workplace after an estimated $75,000 in product was lost. Theft was suspected. The employer was also concerned about other incidents of security, such as assault, threats and vandalism. Eight cameras were installed to address the theft issue, six of which monitored shipping/receiving and exit/entrance areas. A seventh camera was aimed at an entrance/exit area but also captured an employee smoking area and a view of the employee lunchroom. An eighth camera was set up in an area with particularly valuable equipment. A ninth "security-related" camera monitored a production area of the plant.[42]

The arbitrator held that preventing theft was a reasonable purpose for the surveillance at entrance/exit and shipping/receiving areas. The employer has a lawful right to defend its property and surveillance was incidental to that right.[43] He also held that, absent an express term in the collective agreement, there is no blanket prohibition of video surveillance in the workplace.[44] The camera in the production area was found to be an unreasonable invasion of employee privacy and was ordered to be removed as there was no evidence of a significant safety or security issue to be addressed in the production area.[45] Finally, the arbitrator ordered that the camera aimed at the employee entrance near the smoking area be adjusted as much as possible to avoid capturing images of the lunchroom.[46]

---

[39] *Eastmond* at para. 182.
[40] *Unisource* at para. 48; *Pope & Talbot* at para. 31; *Ross* at para. 32.
[41] *Unisource Canada Inc. v. C.E.P. Local 433* (2003) 121 L.A.C. (4th) 437 (Kelleher) ["*Unisource*"].
[42] *Unisource*: The employer did not inform the union or employees of the existence of the last two cameras until shortly before the hearing. The arbitrator, however, chose to analyse the reasonableness of all the cameras as "non-surreptitious" since the union at the time of hearing knew of all the cameras and their locations (at paras. 51, 52). The arbitrator did note that the two surreptitious cameras would not be reasonable because there were alternatives available to surreptitious surveillance (at para. 51).
[43] *Unisource* at paras. 33, 44.
[44] *Unisource* at para. 48.
[45] *Unisource* at para. 56.
[46] *Unisource* at para. 58.

The 1979 decision of *Re Puretex Knitting Co. Ltd and Canadian Textile and Chemical Union*[47] contains an analysis of video surveillance in the workplace which continues to be reviewed, most recently in *Eastmond*[48]. The arbitrator stated that while constant video surveillance of work performance would be regarded as "seriously offensive in human terms"[49], changes in the quality and purpose of the surveillance may lessen its "inhuman" quality, so that less compelling considerations may justify its use.[50] The purpose and scope of surveillance are essential to achieving a reasonable balance between the employee interest in privacy and the employer's commercial interests. More pressing purposes, supported by evidence, may justify greater invasions of privacy while lesser interests may not override the employees' interest in privacy.[51]

A recent arbitral decision has balanced interests and determined that limited video surveillance of a production area is reasonable. In *Pulp, Paper and Woodworkers of Canada Local 8 v. Pope & Talbot Ltd Harmac Pulp Operations*[52], a camera monitored the unloading of barges at a dock. There were no supervisors at the dock, which was separated from main operations by 800 yards, and the employees communicated with management by radio. There were high costs associated with any delay in unloading the barges, and the employer suspected that employees may have been deliberately failing to give supervisors advance notice that unloading was to complete, in order to have extra "downtime".

The camera's use was limited: it was fixed and could not zoom, the employees knew the camera's field of view and could avoid it on breaks. Only the responsible supervisor could view the images, which were monitored but not recorded. The arbitrator acknowledged the enactment of the B.C. *PIPA*, but did not regard the Act as altering the substance of the issues in surveillance cases[53], relying on a contextual and reasonable balancing of the interests in the circumstances.[54] Although he held that the camera was used, at least in part, to monitor productivity of employees[55], the arbitrator found the video surveillance justifiable. The cost of delay, lack of on-site supervision and effective communication with employees made the use of surveillance reasonable to ensure efficient unloading.[56] He held, however, that 24 hour monitoring was not necessary to achieve that purpose.[57] Instead, the arbitrator determined that the camera could be used during emergencies, for 20-minutes at shift changes and periodically during a shift for up to five minutes.[58]

Other PIPEDA Findings

The Federal Privacy Commissioner has recently found video surveillance to be reasonable using a similar analysis.

In Case Summary #264 [59], a locomotive repair company which stored hazardous wastes on site installed video cameras as part of a wider safety and security plan. The cameras were trained on entrance/exit areas, including a ramp on which pedestrian traffic was prohibited. Employees were informed of the cameras and that their purpose was to ensure safety and security. One employee claimed that he was assaulted by a manager at one of the

---

[47] (1979) 23 L.A.C. (2d) 14 (Ellis) ["*Puretex*"].
[48] *Eastmond* at para. 134.
[49] *Puretex* at 29, 30.
[50] *Puretex* at 30.
[51] *Puretex* at 30.
[52] (2003) 123 L.A.C. (4th) 115 (Munroe) ["*Pope & Talbot*"].
[53] *Pope & Talbot* at para. 29.
[54] *Pope & Talbot* at para. 31.
[55] *Pope & Talbot* at paras. 32, 33.
[56] *Pope & Talbot* at paras. 33.
[57] *Pope & Talbot* at para. 34.
[58] *Pope & Talbot* at para. 35.
[59] *PIPED Act* Case Summary #264 "Video camera and swipecards in the workplace", [2004] C.P.C.S.F. No. 9 (QL) (Assistant Privacy Commissioner, February 19, 2004). Online: Quicklaw Database PCCF; Office of the Privacy Commissioner of Canada http://privcom.gc.ca/cf-dc/2004/cf-dc_040219_01_e.asp. (last modified: 22 June 2004) ["Case Summary #264"].

entrance/exit areas. In the course of its investigation, the employer reviewed the videotapes of the entrance and found no evidence of assault. Instead, the employer noted that the employee in question had walked on the prohibited ramp several times, in contravention of a workplace rule and disciplined him for a breach of the *Canada Labour Code*[60].

The Assistant Privacy Commissioner first held that the non-surreptitious surveillance itself was reasonable. The employer had adduced clear evidence of a need to address safety and security issues on site and a reasonable person would consider the company's purposes appropriate. The information collected was restricted to what was necessary to achieve the purposes: the cameras were not trained on areas of production and the employees had no reasonable expectation of privacy at entrance/exit areas.

The Assistant Commissioner then considered whether *PIPEDA* had been breached by using the surveillance to discipline the employee for walking in the prohibited area. An organization, under *PIPEDA*, may use personal information without consent where, in the course of its activities, it becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the law and the information is used for the purpose of investigating that contravention[61]. The Assistant Commissioner held that the information collected about the employee in question was obtained during the course of an investigation and therefore, no consent was necessary for its collection or use in discipline. Accordingly, the video surveillance did not breach *PIPEDA*.

In Case Summary #265[62], the Assistant Privacy Commissioner found that the use of personal information collected by cameras in the workplace was not reasonable when used other than for its intended purpose. A railyard installed a camera to track train movements. The Assistant Commissioner found the cameras appropriate for this original purpose. One day, while observing train movements, a supervisor noticed two employees leaving company property during working hours. He used the zoom function on the camera to determine the employees' identities and they were later disciplined for an unauthorized absence. The employer asserted that there was no "collection" as the camera did not record but was rather a visual aid. It argued that the complainants had no reasonable expectation of privacy, because there was constant pedestrian traffic in the rail yard and the use was an investigation because the complainants were behaving suspiciously on the day in question. The Assistant Commissioner noted that "personal information" is not restricted to recorded information. She found that while the camera was appropriate to enhance workplace safety and track train movements, it was unreasonable to use the cameras to track employee comings and goings when that was not the purpose expressed by the employer for the surveillance. The use of the camera could also not reasonably fall under the investigations exemption under *PIPEDA*. At the time, the supervisor had no other evidence that the employees in question were not authorized to leave nor was there evidence of a significant problem with unauthorized absences generally. The supervisor could have used a less privacy-intrusive way to determine the location of the employees and whether their absence was authorized prior to using the videotape as evidence for discipline. On balance, the use of the cameras to manage workplace performance issues was unreasonable in the circumstances.

The distinction between the cases may lie in the timing, and the resulting reasonableness, of the use. The investigation exception of *PIPEDA* (section 7(2)(a)) also creates a distinction between the circumstances. In Case Summary #264, the company had already commenced an investigation into events involving the employee at the entrance/exit area. In Case Summary #265, there was no investigation that had commenced prior to the observation of the employees.

---

[60] R.S.C. 1985, c. L-2, s. 126(1).
[61] *PIPEDA*, s. 7(2)(a).
[62] *PIPED Act* Case Summary #265: "Video cameras in the workplace" [2004] C.P.C.S.F. No.10 (QL) (Assistant Privacy Commissioner, February 19, 2004). Online: Quicklaw Database PCCF; Office of the Privacy Commissioner of Canada, http://privcom.gc.ca/cf-dc/2004/cf-dc_040219_02_e.asp. (last modified: 22 June 2004) ["Case Summary #265"].

For non-surreptitious surveillance generally, decisions about the reasonableness of surveillance under *PIPA* are likely to develop along the same lines as arbitral jurisprudence and decisions under *PIPEDA*. What is required is a reasonable and contextual balancing of competing interests, taking into account the reasonableness of the purpose and scope of the surveillance.

Surreptitious Surveillance

Arbitrators have drawn a bright line between surreptitious surveillance and surveillance by cameras whose locations and purposes are known to employees.[63]

Surveillance without consent or notification is permitted under the Alberta *PIPA* and B.C. *PIPA* only if it falls under a "no consent" exception.[64] Most arbitral jurisprudence and decisions under *PIPEDA* focus on surreptitious surveillance in the course of investigations.

Surveillance without consent or notification is contemplated under the legislation if it is reasonable for the purposes of an investigation, which includes investigating a breach of an agreement.[65] The OIPCBC Discussion Paper proposes that if an employer engages in surreptitious monitoring, it must demonstrate that:[66]

1. the investigation is based on a reasonable belief that the employment agreement has been breached;
2. there is an ongoing investigation into a specific allegation; and
3. notification would compromise the accuracy or availability of the personal information collected.[67]

PIPEDA Findings

The Federal Privacy Commissioner has stated that surreptitious video surveillance should only be taken as a last resort, even in an investigation. The employer must:

1. initiate surveillance based on substantial evidence of wrongdoing;[68]
2. first try less privacy-invasive ways of gathering the required information;[69] and
3. make the decision to engage in surreptitious surveillance of an employee at a senior management level.[70]

In Case Summary #269[71], an employee reported a number of work-related injuries in the course of his employment. The employee continued to work in positions consistent with his physical limitations but the employer became suspicious of his health claims. He was frequently absent and failed to provide the company with updated medical assessments, despite verbal and written requests. Finally, an independent medical assessment indicated that he might be malingering. The employer commenced surreptitious surveillance of the

---

[63] *Eastmond* at para. 132.
[64] Alberta *PIPA*, s. 14, s. 17 and s. 20; B.C. *PIPA*, s. 12(1), s. 15(1) and s. 18(1).
[65] Alberta *PIPA*, s. 1, s. 14(d), s. 17(d) and s. 20(m); B.C. *PIPA*, s. 1; s; 12(1)(c), s. 15(1)(c) and s. 18(1)(c).
[66] "OIPCBC Discussion Paper" at 3.1.2.
[67] "OIPCBC Discussion Paper" at 3.1.
[68] Anecdotes do not qualify as "substantial evidence": Case Summary #268.
[69] Case Summaries #268 and #269.
[70] Case Summaries #268 and #269.
[71] *PIPED Act* Case Summary #269 "Employer hires private investigator to conduct video surveillance on employee" [2004] C.P.C.S.F. No. 14 (QL) (Assistant Privacy Commissioner, April 23, 2004). Online: Quicklaw Database PCCF; Office of the Privacy Commissioner of Canada, http://privcom.gc.ca/cf-dc/2004/cf-dc_040423_e.asp. (last modified: 22 June 2004) ["Case Summary #269"].

employee to determine if he was being truthful about his physical limitations. After reviewing videotape showing the employee performing activities that contradicted his claims of incapacity, the employer concluded that the employee was not being truthful. Emphasizing that video surveillance should only be used as a last resort in an employee investigation, the Assistant Privacy Commissioner found that the employer had substantial evidence of malingering prior to engaging in surveillance. The employer had "reasonable and probable cause" to believe the employee was violating the employment contract. The employee was uncooperative and the employer was unable to get the information it required in a less privacy-invasive manner. The Assistant Commissioner held that the video surveillance was reasonable but noted that the decision to engage in surreptitious video surveillance of an employee should be made by senior management.

Case Summary #268[72] also considered the reasonableness of surreptitious surveillance in an investigation. A manager of a company engaged in air travel attached a voice recording device to the underside of a table in the smoking lounge. Both employees and customers used the smoking lounge, but at this particular time, the manager expected to record only the conversations of certain employees. The manager suspected the employees of wrongdoing, but evidence was obtained only after the surveillance had taken place. The Assistant Privacy Commissioner found that, since the voice recording had been erased by one of the complainants, it was not proved that there was a collection of personal information. However, the Assistant Commissioner stated in *obiter* that, if the information had been recorded, the investigation would not have been reasonable under *PIPEDA*. She stated that an organization must have "substantial evidence to support the suspicion that the employee is engaged in wrongdoing or that the relationship of trust has been broken, must be able to show that it has exhausted all other means of obtaining the information that it required in less privacy-invasive ways, and must limit the collection to the purposes to the greatest extent possible."[73] There was, at the time of the recording, no substantial evidence of wrongdoing, only suspicion by the supervisor and "anecdotes". There were less privacy-intrusive methods of investigating the incidents. Furthermore, the recording was highly indiscriminate, taking place in a room accessible to many other individuals. The Assistant Commissioner stated that a decision to conduct surreptitious surveillance of employees in an investigation should be made at a very senior level of management.

Arbitral Jurisprudence

Similarly, arbitral jurisprudence has generally considered surreptitious surveillance to be reasonable if:[74]

(a) there is a substantial problem;

(b) there is a strong possibility that surveillance will be effective; and

(c) there is no reasonable alternative to surreptitious surveillance.

Notably, the factors used by arbitrators to assess surreptitious surveillance are essentially the same as those considered by arbitrators to assess non-surreptitious surveillance. However, the difference lies in the higher threshold for reasonableness when the surveillance is surreptitious[75]. In the recent adjudication of a complaint of unjust dismissal under the *Canada Labour Code* in *Ross v. Rosedale Transport Ltd.*[76], the adjudicator analysed the reasonableness of surreptitious surveillance of an employee under *PIPEDA*. The employee had worked as a driver

[72] *PIPED Act* Case Summary #268 "Electronic monitoring does not yield any information, but practice is strongly discouraged" [2004] C.P.C.S.F. No. 13 (QL) (Assistant Privacy Commissioner, April 12, 2004). Online: Quicklaw Database PCCF; Office of the Privacy Commissioner of Canada, http://privcom.gc.ca/cf-dc/2004/cf-dc_040412_e.asp. (last modified: 22 June 2004) ["Case Summary #268"].
[73] Case Summary #268, "Further Considerations".
[74] *Unisource* at para. 48.
[75] *Ross v. Rosedale Transport Ltd.* [2003] C.L.A.D. No. 237 (Brunner) at para. 32 ["*Ross*"]; *New Flyer Industries v. CAW Canada Local 3003*, February 17, 2003 (Peltz) at para. 4.
[76] *Ross.*

for nine years and was described as a "good employee" with no prior disciplinary or adverse work record.[77] The employee sustained a back injury at work and was subsequently accommodated by the employer in clerical and administrative positions. As time progressed, however, the supervisor suspected that the employee was malingering. Four months after his injury, and still working in the accommodated position, the employee took a vacation during which time he and his family were moving. The supervisor hoped to obtain video surveillance evidence that the employee was malingering by video taping the move. The surveillance recorded the employee moving furniture, which appeared contrary to his claims of injury. The employee alleged that the surreptitious surveillance collected his personal information without his consent and was therefore contrary to *PIPEDA*. The adjudicator stated that general arbitral principles on surreptitious video surveillance used prior to the enactment of *PIPEDA* are also expressed in the circumstances set out in section 7(1) which permits collection of personal information without knowledge or consent.[78] The adjudicator analysed the reasonableness of the investigation, using those general arbitral principles. The adjudicator found that the surveillance was not reasonable for the purpose of investigating Ross' injury. There was no evidence of dishonesty prior to the initiation of surveillance, only suspicion on the part of the employer.[79] The adjudicator held that the employer had other ways to verify the employee's injuries rather than engaging in surreptitious surveillance, such as asking for an independent medical assessment. The adjudicator found that the employer's surveillance was like "casting an electronic web" to see if the employer could catch something. The investigation by surreptitious surveillance was not reasonable and was inadmissible to prove cause for dismissal.[80]

While a reasonable purpose and reasonable scope will always be part of the test for reasonableness under personal information protection legislation, the analysis will differ between surreptitious and non-surreptitious surveillance of employees. There will likely to continue to be a greater threshold than for non-surreptitious surveillance, requiring evidence of a substantial problem and a greater evaluation of alternatives.

E-mail and Internet Monitoring

There are few cases discussing e-mail and Internet monitoring of employees, but one would expect a consideration of the privacy issues under the Alberta *PIPA* and B.C. *PIPA* to follow the analysis applied to video surveillance.

The principles affirmed in *Eastmond* and expressed by the federal Privacy Commissioner with respect to video surveillance may also be applied to the determination of whether electronic monitoring of employee e-mail and Internet use is reasonable under privacy legislation. Both the purpose and scope of monitoring must be reasonable, but a line will again be drawn between non-surreptitious and surreptitious electronic monitoring.

Disclosed, Non-Surreptitious Surveillance

For non-surreptitious monitoring, reasonableness will likely depend on the reasonable balancing of employer interests and employee privacy rights in all the circumstances, taking into account the following factors:

1. Is it necessary for a legitimate or reasonable business interest?
2. Is the information collected by surveillance only that necessary to achieve the intended purpose?
3. To what extent is employee privacy affected?
4. Were alternatives considered and will they be effective?

[77] *Ross* at para. 6.
[78] *Ross* at para. 34.
[79] *Ross* at para. 35.
[80] *Ross* at para. 36.

Employers may have a number of legitimate reasons to monitor e-mail and Internet use (including "theft of time", other productivity issues and workplace harassment). However, reasonableness requires not only a reasonable purpose, but also a reasonable scope. Like video surveillance, the scope of the monitoring must be tied to the intended purpose. If an employer is concerned with "theft of time", effective monitoring may only require a review of the addresses to which e-mails are being sent, the quantity of e-mails, the headings of e-mails or names of websites visited. If the employer is concerned with overloading the server or network, only the size of the e-mails and attachments may need to be monitored.

Like video surveillance, the reasonableness of e-mail and Internet monitoring at work will likely depend on the reasonable balancing of interests of the employee and employer. A greater scope of monitoring will likely require a more substantial employer concern.

Judicial and Arbitral Jurisprudence

The judicial and arbitral decisions have focused on the employee's reasonable expectation of privacy in the circumstances, looking at e-mail policies published in the workplace, among other circumstances. The legitimacy of monitoring is evaluated based on whether there is a reasonable expectation of privacy in work e-mail and Internet use.

In *Milsom v. Corporate Computers Inc.*[81], the Court held that because there was no e-mail policy in the workplace, an employee had no reasonable expectation of privacy in his work e-mail and the employer was entitled to introduce it as evidence of poor performance.[82] The Court, referring to decisions of United States courts, stated that even where an e-mail policy outlines some employee privacy rights, there may be no reasonable expectation of privacy when the contents of e-mails are unprofessional, offensive or where access by the employer is part of an investigation of illegal activity.[83] An employee may also have no reasonable expectation of privacy, regardless of a policy, if the e-mail is sent and received using corporate assets.[84]

In *Camosun College v. C.U.P.E. Local 2081*[85], the arbitrator also found that the employee had no reasonable expectation of privacy in work e-mail or a chat group for Union members on the employer's computer network. The arbitrator reasoned that there could be no reasonable expectation of privacy where it was well-known that the message could be easily copied by any subscriber to the e-mail group and forwarded without the knowledge of the sender.

In other cases, such as *Owens-Corning Canada Inc. v. C.E.P. Local 728*[86] and *Briar v. Canada (Treasury Board)*[87] it was held that there was no reasonable expectation of privacy in work e-mail because the employees were warned that inappropriate e-mails were not tolerated and could be subject to monitoring and that discipline might follow a breach of the company standards.

Under personal information protection legislation, the focus is on the collection, use and disclosure of personal information, not simply private information. Previous judicial and arbitral decisions may be helpful in determining reasonableness by discussing the extent to which employee privacy is affected. However, their discussions of reasonableness do not generally address the collection of personal information and the obligation of employers to limit their collection and use of personal information. Specifically, case law and arbitral analysis may not address

---

[81] [2003] A.J. No.516, 2003 ABQB 296 ["*Milsom*"].
[82] *Milsom* : The Court held that poor performance is rarely cause for dismissal and despite the e-mail evidence, Milsom should have only received a warning (at paras. 38, 50).
[83] *Milsom* at para. 40.
[84] *Milsom* at para. 46.
[85] unreported (November 15, 1999), Doc A-321/99 (B.C. Arb. Bd) (Germaine) at para. 12 ["*Camosun*"].
[86] (2002) 113 L.A.C. (4th) 97 (Price) ["*Owens-Corning*"].
[87] (2003) 116 L.A.C. (4th) 418 (Taylor) ["*Briar*"].

questions of whether the monitoring is reasonably necessary, whether there are alternatives available to the monitoring and the reasonable scope of investigation in the circumstances. All these considerations will be key issues under the legislation.

Reasonable monitoring in accordance with the personal information protection legislation should only collect and use information that is necessary to achieve a reasonable business purpose. Reasonableness will also depend on the extent to which the monitoring affects employee privacy rights. While an employee's reasonable expectation of privacy will likely be diminished at work and using work e-mail, there may remain a reasonable expectation of some privacy in employee e-mail[88]. Employers should make clear to employees what their reasonable expectation of privacy should be, notifying them of the purpose and scope of e-mail or Internet monitoring. Individual passwords and security features may give the employees the impression of confidentiality and privacy which should clearly be dealt with in the appropriate policies. In *Briar*[89], the adjudicator held that the employees had no reasonable expectation of privacy in their work e-mail where the prison had a clear policy against use of the e-mail system for unacceptable purposes. The employees received a warning each time they logged in that the system was monitored in accordance with the policies.[90]

Unless it is limited by the employer's express policy, an employee's reasonable expectation of privacy will likely increase for e-mails the employee writes during "off-work" hours (for example, during breaks and lunch) and for e-mails written from a private ISP account. In *Owens-Corning*, it was not reasonable for the employer to review the employee's personal webmail account while investigating improper use of work e-mail[91].

Notwithstanding the absence of a similar analysis under arbitral decisions, it is reasonable to expect that the scope of monitoring must be closely tied to the purpose of monitoring, collecting and using only information necessary to achieve the employer's purpose. The employer may also have to consider whether there are any reasonable or effective alternatives to surveillance.

Surreptitious Monitoring

An employer may monitor e-mail and Internet use of an employee without notification or consent if it is reasonable for an investigation or falls under another "no consent" exception.[92] As with video surveillance, for an investigation of an employee's e-mail or Internet use to be reasonable, the following may be required:

(a) evidence of wrongdoing prior to initiating the investigation. Independent evidence in the arbitral jurisprudence commonly takes the form of complaints or observations by coworkers, supervisors or customers;

(b) the monitoring should be restricted to only that necessary to achieve the employer's purpose; and

(c) there should be no reasonable or equally effective alternatives to the surreptitious monitoring.

In *Owens-Corning Canada Inc.*[93], prior to initiating surveillance, the employer had reason to suspect both a widespread problem within the company of inappropriate e-mail and Internet use by employees, and evidence that the employee, specifically, was using his e-mail and Internet privileges inappropriately[94].

---

[88] In *R.. v. Weir* [1998] A.J. No. 155 (Alta Q.B.), affirmed 2001 ABCA 181, a decision involving criminal charges and not work-related, the Court held that there ought to be a reasonable expectation of privacy in e-mail in a personal account sent via the Internet at para. 56.
[89] *Briar.*
[90] *Briar* at para. 51.
[91] *Owens-Corning* at para. 78
[92] Alberta *PIPA*, s. 14, s. 17 and s. 20; B.C. *PIPA*, s. 12, s. 15 and s. 18.

That same case also illustrates how an excessive scope of investigation can result in monitoring being held to be unreasonable. In *Owens-Corning*[95], an employee received numerous personal e-mails into his work e-mail account each day. However, he usually forwarded the personal e-mails to a personal webmail account and did not send them to anyone inside or outside the company. After learning that the employee had been accessing the Internet using another employee's ID, the employer began looking at "computer reports" which stated which computer operator visited which internet sites for how long. The employer's concern was initially one of security. However, the employer had also recently implemented a non-harassment policy in response to a widespread problem of inappropriate e-mails being sent by employees. After looking at the computer reports, the employer suspected the employee of visiting inappropriate websites. The employer reviewed the employee's work e-mail and accessed his personal webmail account without his consent. The arbitrator found that while the employee had no reasonable expectation of privacy in his work e-mail, the investigation of his personal webmail account was unreasonable.[96] The employee had a reasonable expectation of privacy in his personal e-mail account, which was in not connected to his employment.[97]

There has been little discussion in the jurisprudence of the need to consider to alternatives to surreptitious e-mail and Internet use monitoring. The analysis may be similar to that set out with respect to video surveillance.

Assessing an Employer's Right to Monitor

Much like the duty to accommodate, the assessment of whether an employer may exercise a right to monitor depends on the particular circumstances of each case. Compliance with privacy legislation, reasonableness and appropriate balancing of the employee's right to privacy will be examined.

Decisions on other forms of employee surveillance can be used to determine how an arbiter will view a planned monitoring or surveillance program. and legal advice is definitely recommended. Some of the

Is the Monitoring Open or Surreptitious?

Surreptitious surveillance is the most intrusive type of monitoring and therefore has the greatest potential to undermine employee privacy rights. However, where employees give express consent to employers regarding specific monitoring, any such monitoring would likely not conflict with the employees' privacy rights. It is noteworthy that adjudicators have found that simply accessing a computer system that the employer wholly owns and viewing saved files may not constitute surreptitious.[98]

What is the Employer's Objective?

Employers may monitor employees' computers to address system maintenance issues, to deter or to address certain misconduct (accessing objectionable material on the Internet or from other sources), or in response to a complaint of discrimination, theft, threats or breach of the employment agreement. Focused monitoring, particularly in response to actual or reported problems, will generally be seen as being a legitimate exercise of the employer's right to manage the workplace and will be more likely to withstand challenge than monitoring activity that investigates all aspects of employee productivity, character or conduct.

---

[93] *Owens-Corning*.
[94] *Owens-Corning* at paras. 24, 34-36.
[95] *Owens-Corning*.
[96] *Owens-Corning* at para. 77.
[97] *Owens-Corning* at para. 78.
[98] For example, see *Re Insurance Corporation of B.C. and Office and Technical Employees Union, Local 378* (Unreported, January 27, 1994).

What is Being Monitored?

Where an employer has designated particular directories for employee personal files, or where a computer file is clearly marked as "personal", a decision to view such files may be considered more intrusive than reviewing clearly work-related files.[99] Distinctions may also be drawn based on the physical location of a computer or a place being monitored. In *Pacific Northwest Herb Corp. v. Thompson*,[100] the employer accessed a computer storing the disputed files, which had been used by the former employee at home. The Court found that the employee was presumed to have had authority to use the computer for personal purposes under the circumstances, especially since he was never informed otherwise. A clear-cut problem is where monitoring or surveillance is conducted at or near employee washrooms, change rooms, lunch rooms or other places where an employee has an expectation of privacy greater than places they regularly perform work. In such places, employers must show a pressing need for monitoring or surveillance.

What Information will be Collected

Monitoring employee computer use to determine the volume or size of files received or sent, addresses to which e-mail is being sent, or the amount of time spent surfing the Internet will generally be characterized differently than a more intensive search that reviews the content of e-mails or files. Video monitoring that is not reviewed unless an incident is reported, particularly where the tape is erased or taped over within a day or two, will not be considered as intrusive as video monitoring that is reviewed as a matter of course. Monitoring that collects identifiable information about employees will require greater planning and precaution as additional considerations regarding use, storage and retention in accordance with applicable privacy legislation.

Additional Considerations

In addition to the factors, above, the increase of privacy legislation may result in more limitations being placed on an employer's ability to restrict employee privacy expectations. As early as 1974, the Supreme Court of Canada decided that an arbitrator may consider the application of statutory law when interpreting collective agreements, even if the statute is not referenced in the collective agreement.[101] Accordingly, it is to be expected that arbitrators will increasingly be called upon to interpret and apply privacy legislation in workplace disputes, particularly where the dispute involves employee monitoring or surveillance.

An adjudicator's balancing of management's interests and employee privacy will be influenced by various factors, including: whether the technology being used for inappropriate conduct was provided by the employer or by a private party; whether the inappropriate use extends outside the immediate workplace; the potential liability and damage that could be caused by the inappropriate conduct; whether the inappropriate conduct occurred on the employee's time or on company time; and whether the employee knew or ought to have known better.

In analyzing whether an employer's search or investigation was acceptable, adjudicators will focus on: whether employees had notice of the policy supporting the search; the reasonableness and clarity of the policy; the reasonableness and consistency of the administration of the policy; and the reasonableness of the employer's grounds for the search. Reasonable searches, supported by policy or circumstances, will be upheld by courts and

---

[99] Morgan, Charles. "Employer Monitoring of Employee Electronic Mail and Internet Use" (1999) 44 *McGill L.J.* 849 at para. 73.

[100] (December 6, 1999), Vancouver C984823 (B.C.S.C.).

[101] *McLeod v. Egan* (1974), 46 D.L.R. (3d) 150, and subsequently reinforced in *Parry Sound (District) Social Services Administration Board v. O.P.S.E.U., Local 324*, 2003 SCC 42.

.

adjudicators if the probative value of the information gathered exceeds the degree of intrusiveness into the employee's privacy rights.

A high-profile example of an employer investigation being undermined by some of the above factors is what happened at Ontario's Ministry of Natural Resources ("MNR") in 2001. The MNR discovered a few employees had images of nude women on their computers. At the same time, the MNR received a complaint from Chrysler Canada that two of its employees had allegedly received inappropriate e-mail messages from MNR staff on two occasions. At the conclusion of the investigation, 189 employees were found to have inappropriate material in their work e-mail accounts. About half had limited images in their e-mail accounts and had not distributed them. These employees were coached but were not disciplined. The other half, approximately 90 employees, had large volumes of pornographic materials in their e-mail accounts and/or had distributed such materials. Eventually 66 employees were disciplined. The discipline ranged from written reprimands, varying suspensions, and dismissal of six employees who were considered the worst offenders. The material in the possession of these employees was considered extremely offensive, and was described as degrading, dehumanizing and violent by investigators. MNR had a Workplace Discrimination and Harassment Policy and Information Technology policy and each employee's log-in protocol included a warning that popped up on the computer screen explaining what constituted improper computer use.

At arbitration, the Ontario government was ordered to reinstate the six dismissed employees.[102] Arbitrator Petryshen found MNR did not have just cause to discharge the employees even though they exchanged very offensive pornographic materials via their workplace e-mail system contrary to workplace policies. After the 43-day hearing which was heard over four years, he concluded that the government "conducted a careful and extensive investigation and that the disciplinary process was handled in a fair and professional manner." Despite this finding, Mr. Petryshen reinstated the grievors because the problem of e-mail abuse was widespread and inappropriate material was found in the accounts of numerous managers and human-resources employees, including men and women, suggesting that the workplace culture condoned such activity. Also, all of the grievors were first-time offenders and progressive discipline had been ignored.

Privacy Problem Prevention

Employers can avoid potential problems arising out of employees' privacy rights in the workplace by taking some preliminary steps and considering the following points:

- Establish a comprehensive written policy addressing what expectations employees should have regarding their right to privacy and bring that policy to the attention of all employees. Such a policy should describe exactly what measures are or may be taken by the employer to monitor the employees' activities. For example, employees should be informed that their e-mails may be monitored from time to time or that surveillance cameras have been installed to ensure the safety of workers.

- Ensure that any policy statement describes the purpose of any surveillance or monitoring, and includes a statement of what appropriate uses can be made of the employer's resources, such as telephones or computer programs. Care must be taken not to describe too broad or too narrow a purpose.

- Consider whether the written policy should also include the employee's specific consent to surveillance and monitoring. By obtaining such consent, the employer will be helping to ensure that the employee's reasonable expectations of privacy correlate with the employer's intentions of exercising their right to reasonably monitor workplace activities.

[102] *Ontario Public Service Employees Union (Hastie et al.) -and- The Crown in Right of Ontario(Ministry of Natural Resources)*, (Ken Petryshen, June 18, 2004, unreported).

- Consider any rights or prohibitions provided for in existing collective agreements or employment contracts, before taking any steps to introduce any policies or to introduce surveillance mechanisms into the workplace.

- If video surveillance is to be introduced, remember that case law indicates that an employer must have reasonable grounds to establish video surveillance, and that the intrusiveness of any such surveillance should be kept to a minimum. Accordingly, rotating cameras and open surveillance are considered preferable to fixed cameras and surreptitious surveillance.

- Remember that the employer must have even more compelling grounds to engage in any surveillance *outside of the workplace*, as an employer will be extending his right to know beyond the place of employment and into the employee's personal life.

Prevention: Introducing an Internet/E-mail Policy

An effective e-mail and Internet policy should include:

- a statement that the equipment is provided for business use;

- express parameters regarding personal use (for example, "no personal use is permissible" or "personal use should occur during breaks only and should be responsible");

- express limitations on the type of material which may be accessed or sent (for example, no criminal material and no sexist, racist, sexually offensive; obscene or violent materials);

- guidelines for acceptable personal use which include a statement concerning the type or nature of content which constitutes inappropriate usage, including verbal abuse, defamation, sexually explicit, or derogatory, obscene or other offensive communications;

- a statement prohibiting any employee from receiving, viewing, accessing or sending any materials which are contrary to the *Human Rights Code* or the *Criminal Code*;

- a statement that employees should have no expectation of privacy and that the company may monitor and review the employee's use, including opening e-mail messages;

- a requirement that employees must comply with all copyright, patent and trademark rights, including a prohibition on any unauthorized downloading, transfer or other use of such material;

- a prohibition on the use of the electronic networks for the purposes of soliciting or otherwise advancing any personal business or activity of an employee, such as political or religious solicitation;

- other rules or practices recommended by your IT manager to ensure the effective and safe functioning of the system (such as virus checks and password rules); and

- a warning that employees will be subject to discipline up to and including termination of employment for violations of the policy.

Steps should be taken to ensure that the policy is brought to the employee's attention and that the employer can prove that the employee was aware of the policy. Proof may be obtained by having employees sign and return a copy of the policy which is then kept in their personnel file or by having employees perform an electronic acknowledgement when they log-on, an electronic copy of which is preserved.

Some employers have taken the additional step of having a "warning" banner appear on the computer screen every time an employee logs on, with text to the effect that the system is intended only for use by authorized individuals for business purposes only and in accordance with the employer's electronic network policy.

Employers who are bound by a collective agreement may implement an Internet/e-mail policy on a unilateral basis as part of management rights, in accordance with the "*KVP* criteria"[103], which requires that the rule or policy must:

- not be inconsistent with the terms of the collective agreement;
- not be unreasonable;
- be clear and unequivocal;
- be brought to the attention of the employee affected before the company can act on it;
- be consistently enforced from the time it was introduced; and
- make employees aware that breach of the rule can result in discipline including discharge.

The Criminal Code

When considering monitoring the e-mail use of employees, employers should be aware that there are *Criminal Code* provisions regarding interception of private communications. Section 184(1) of the *Criminal Code* states that "every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years."[104] A "private communication" is "any oral communication or any telecommunication…made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it…"[105]

Section 184(1) does not apply to a person who has the consent to intercept, express or implied, of the originator of the private communication or of the person intended by the originator thereof to receive it.[106] An employer must carefully consider whether it has the appropriate consent.

There is an argument that e-mail is not "private", especially for messages sent at work or from a work e-mail account. Verbal pager messages, for example, have been held not to be private communications where the pager plays the message so that anyone in the vicinity of the recipient can hear it.[107] A court may find that, due to the use of passwords and the usual expectation of people that their e-mails will not be intercepted, even an e-mail sent from work is a "private" communication. Even if an employee has no reasonable expectation of privacy in work e-mail, a third party may have a reasonable expectation of privacy in that e-mail message. Any monitoring of computer systems and e-mails should be reviewed in light of the *Criminal Code* provisions and relevant case law.[108]

---

[103] *RE KVP Co. and Lumber and Sawmill Workers' Union, Local 2537* (1965), 16 L.A.C. 73, at p. 85.

[104] *Criminal Code*, R.S.C. 1985, c. C-46, s. 184(1); see also s. 193 which makes it an offence to use or disclose information from intercepted private communications, subject to certain exceptions.

[105] *Criminal Code*, s. 183.

[106] *Criminal Code*, s.184(2)(a).

[107] *R. v. Lubovac* (1989) 101 A.R. 119 (Alta. C.A.).

[108] For an extensive discussion of e-mail and Internet monitoring in the workplace, see Charles Morgan (1999) "Employer Monitoring of Employee Electronic Mail and Internet Use", (1999) 44 McGill L.J. 849.

Conclusion

Personal information protection legislation focuses employers' attention on a new legislated balance between legitimate business interests and employees' privacy interests. Despite new obligations and concepts of consent and access, the Alberta *PIPA* and B.C. *PIPA* import some time-tested principles. The concepts of "reasonableness" and the "reasonable person" are integral to the legislation and invite reference to previous arbitral jurisprudence on the reasonableness of surveillance and monitoring in the workplace. *PIPEDA* decisions, too, assist in predicting the likely analysis of surveillance and monitoring under the new personal information protection legislation. *PIPEDA* findings use similar, if not identical, considerations as arbitral decisions to find a reasonable balance between employer interests and employee personal information protection. *PIPEDA* findings articulate other obligations, such as restricting purposes and requiring senior-level decision-making. New privacy legislation responds to the changing demands and concerns in society and the workplace regarding privacy and attempts to address the challenges of doing business and employing individuals in what has been referred to as the "Information Age".