International Association of Judges (Dakar, Senegal)

Fourth Study Commission
Public and Social Law

QUESTIONNAIRE 2010: Aspects of data protection in employment relationships

Responses[1] by Justice Judith A. Snider, Federal Court, Canada[2]

TABLE OF CONTENTS

[1] The views expressed are those of the author and do not necessarily reflect the views of the Federal Court or its judges.

[2] The author acknowledges the assistance of Ms. Diana Tseng, Law Clerk, in the preparation of these responses.

I) PREFACE

In approaching the questions for this Fourth Study Commission, one must appreciate that Canada is a complex federal state. Legislative power are divided between federal and provincial governments, and each derives jurisdiction from *The Constitution Act, 1867* (U.K.), 30 & 31 Victoria, c. 3 (*Constitution*). Pursuant to s. 92(13) of the *Constitution* (property and civil rights), the provinces have sole jurisdiction over regulation of employment. Consequently, each province within Canada has enacted legislation to address employment matters within its territory. There is, however, a significant exception which occurs where the federal government is regulating labour and employment matters within a "federal work, undertaking or business" (see Collin H.H. McNairn, *A Guide to the Personal Information Protection and Electronic Documents Act* (Markham: LexisNexis Canada Inc., 2010) at 13). The federal government can legitimize its control of employment and privacy issues through s. 91(2) of the *Constitution* (the regulation of trade and commerce), or under the residual power of "Peace, Order and Good Government of Canada". On a very general level, federal oversight of employment matters does not differ significantly from that of individual provinces. Accordingly, the answers contained in this paper focus on legislative schemes at the federal level.

In January 2001, the Canadian Parliament implemented a new data protection law, the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (*PIPEDA*). There is a strong priority on privacy and information rights in Canada. Even though it is only in its infancy stage, *PIPEDA* has been classified "as a fundamental law of Canada just as the Supreme Court of Canada ruled the federal *Privacy Act* enjoyed quasi-constitutional status" (*Eastmond*, above, at para. 100). *PIPEDA* regulates the collection, use and disclosure of personal information within the private sector – this includes the employment context if the employer is "federal work, undertaking or business" (McNairn, above, at p. 9; *PIPEDA*, s. 4(1)(b)). While the statute is recognized as "quasi-constitutional", it does not make privacy rights absolute. Rather, *PIPEDA* attempts to balance the privacy interests of individuals, against the business or security needs of the employer (*PIPEDA*, s. 3; McNairn, above, at p. 7).

While implemented in 2001, *PIPEDA*'s roots anchor back to the 1980s and Canada's membership in the international Organization for Economic Co-operation and Development (OECD). In 1980, OECD developed the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (23 September 1980) (*OECD Guidelines*). Canada signed onto the *OECD Guidelines* in 1984 (Lisa M. Austin, "*Is Consent the Foundation of Fair Information Practices? Canada's Experience under PIPEDA*" (2006) 56 Univ. of Toronto L.J. 181 (QL)). The *OECD Guidelines* stipulate a number of fair information principles that have influenced Canada's data protection laws. The fair information principles were incorporated into Canada's *Model Code for the Protection of Personal Information: A National Standard of Canada*, CAN/CSA-Q830-96 (*Model Code*). The *Model Code* is our country's first national articulation of fair information practices and principles (Austin, above). The *Model Code* reflects "the agreement of a wide range of governmental and industry representatives who made up the Technical Committee on Privacy of the Canadian Standards Association" (McNairn, above, at p. 3). In 2001, the *Model Code*'s fair information principles became an integral part Canada's data protection law - *PIPEDA*.

PIPEDA's legislative scheme is divided into two parts: statutory provisions, and Schedule 1 (the Schedule). The Schedule directly incorporates the *Model Code*. Although the Schedule retains the fair information principles, the statutory provisions in *PIPEDA* do not. Accordingly, the Schedule is to be interpreted with the qualifying provisions from the body of *PIPEDA* (McNairn, above, at p. 4-5; *Eastmond v. Canadian Pacific Railway*, 2004 FC 852, 254 F.T.R. 169 at paras. 183-186 (*Eastmond*)).

In the context of employment relations, the Schedule and its fair information principles are summarized as follows (see **Appendix A** for full text):

> **4.1 – Accountability**: Employers are responsible for any personal information under their control, shall designate individuals who are accountable for the employers' compliance with *PIPEDA*, and shall implement policies and practices relating to *PIPEDA*.
>
> **4.2 – Identifying Purposes**: Employers shall identify the purposes for which personal information is collected. This is to be done at or before the time of collection.
>
> **4.3 – Consent**: Knowledge and consent of the employee is required (except where inappropriate) for the collection, use or disclosure of his or her personal information.
>
> **4.4 – Limiting Collection**: The collection of personal information shall be limited to what is necessary for the purposes identified by the employer. As well, information shall be collected fairly and lawfully.
>
> **4.5 – Limiting Use, Disclosure and Retention**: Except with the consent of the employee(s) or as required by law, personal information shall not be used or disclosed for purposes other than those identified by employers during the collection process. As well, personal information shall be retained only as long as necessary to fulfill the stated purposes.
>
> **4.6 – Accuracy**: Personal information collected must be as accurate, complete, and up-to-date as is necessary for the stated purposes.
>
> **4.7 – Safeguards**: Personal Information shall be protected by security safeguards that are appropriate and proportionate to the sensitivity of the information.
>
> **4.8 – Openness**: An employer's policies and practices, relating to the management of personal information, must be readily available to their employees.

> **4.9 – Individual Access**: Upon request, an employee must be informed of the existence, use, and disclosure of his/her personal information, and must be given access to that information. As well, the employee can challenge the accuracy and completeness of the information, and request appropriate amendments.
>
> **4.10 – Challenging Compliance**: Employees can challenge their employer's compliance with the principles and *PIPEDA*. Employers must put accessible and simple procedures in place to receive, investigate, and respond to complaints about their policies and practices.

The language of *PIPEDA* and the Schedule cover different types of electronic personal information. However, *PIPEDA*, administered by the Office of the Privacy Commissioner of Canada (Privacy Commissioner), regulates an employer's use of camera surveillance.

II) QUESTIONS & ANSWERS

1. Are there explicit legal provisions concerning camera surveillance especially at working places? Are there collective agreements defining the circumstances and conditions for the introduction and use of camera surveillance?

Short answer: *PIPEDA does not explicitly deal with camera surveillance in the work place. However, ss. 5, 7 and the Schedule have been cited by the Privacy Commissioner, the Courts and labour arbitrators when disputes arise on camera surveillance. Collective agreements vary widely on the treatment of camera use. Some explicitly address the issue, while others are completely silent. The existence or lack of provisions about camera use affects the forum where complainants can seek remedies.*

Are there explicit legal provisions concerning camera surveillance especially at working places?

There are no explicit legal provisions in *PIPEDA* that deal with camera surveillance. However, the regulation of camera use has been considered by the Privacy Commissioner and labour arbitrators, and in jurisprudence of the Federal Court of Canada (Federal Court). Of particular importance are ss. 5 and 7 of *PIPEDA.*

According to s. 5(3) of *PIPEDA*: "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances." This "reasonable purpose" provision has been interpreted by the Privacy Commissioner and the Federal Court to encompass four factors (*Eastmond*, above, at paras. 126-127):

a. Is camera surveillance and recording necessary to meet a specific [employer] need;

b. Is camera surveillance and recording likely to be effective in meeting that need;

c. Is the loss of privacy proportional to the benefit gained; and

d. Is there a less privacy-invasive way of achieving the same end?

Furthermore, the Schedule and its principles (see page above) are also applicable to the context of camera surveillance use. Principle 4.3, regarding consent, is often raised. The general principle is that consent is required in order to collect personal information on video cameras. However, under s. 7, employers may not need the consent of their employees under certain enumerated situations.

These provisions and principles will be discussed in more detail in other parts of this document.

Are there collective agreements defining the circumstances and conditions for the introduction and use of camera surveillance?

Collective agreements vary widely. One of the key issues with provisions about camera surveillance is that of forum to seek remedies. The question is whether the essence of the dispute arises from the collective agreement (*Eastmond*, above, at para. 99). Where there are explicit provisions in the collective agreement, conflicts are brought before labour arbitrators. Where there is no such provision, an arbitrator likely has no jurisdiction, and employees must seek remedies from the Privacy Commissioner or the Courts (*Eastmond*, above, at para. 115). Where the situation is more nebulous, s. 13(2)(a) of *PIPEDA* gives the Privacy Commissioner a discretion to investigate a complaint, or defer it to an arbitrator where a grievance is more appropriate.

On one end of the spectrum, some provisions are explicit on the use of camera surveillance. See, for example, the 2004 to 2009 collective agreement between Westfair Foods Ltd. Real Canadian Superstore Distribution Centre & Extra Foods in British Columbia AND United Food & Commercial Workers Union, Local 247 (A.F.L. – C.I.O.):

> 26.5 Video Surveillance
>
> Video surveillance is a valuable resource that can be used to help safeguard employees and customers as well as protect both Company and employee assets. Within the confines of the law, the Company will utilize video surveillance equipment on its property.

Here, a labour arbitrator will probably have exclusive jurisdiction over a dispute, and the Court or Privacy Commissioner is likely to decline jurisdiction over the matter (see *Eastmond*, above, at para. 101; *L'Écuyer v. Aéroports de Montréal*, 2003 FCT 573, [2003] F.C.J. No. 752 (QL)).

On the opposite end, other collective agreements are completely silent on camera use. This occurred in *Eastmond* (above). Employees of the Canadian Pacific Railway (CP) filed a grievance because of CP's camera use. However, employees could only invoke articles 28

(which deals with grievances) and 43 (which deals with human rights and harassment) (*Eastmond*, above, at para. 112). The grievance was denied because nothing in the collective agreement dealt with video surveillance; thus, employees had to file a complaint with the Privacy Commissioner (*Eastmond*, above, at paras. 113-114).

At the middle of the spectrum, some collective agreements can be interpreted to imply regulation over the use of camera surveillance. See, for example, the terms at issue in *United Food and Commercial Workers Union Local 1000A v. Janes Family Foods*, 2006 CanLII 36615 (ON L.A.) at p. 3-4 (*Janes Family Foods*):

> **ARTICLE 4 – MANAGEMENT RIGHTS**
>
> **4.01** Except as, and to the extent specifically modified by this Agreement, all rights and prerogatives which the Company had prior to the execution of this Agreement are retained by the Company and remain exclusively and without limitation within the rights of the Company and its management. Without limiting the generality of the foregoing, the Company's rights shall include:
>
> (a) The right: to maintain order, discipline and efficiency; to make, alter and enforce, from time to time, rules and regulations, policies and practices, to be observed by its employees; to discipline and discharge employees for just cause. The Union Chairperson shall be notified of any changes to or the introduction of any rules and regulations. In the event the Union disputes the reasonableness of such rules and regulations, the Union shall have the right to file a policy grievance in respect hereof pursuant to the provisions of Article 7.04 of this Agreement. Such grievance shall specify the rule or rules being disputed and the grounds upon which such rule or rules is or are being disputed.

In this case, the arbitrator determined there was no clear provision about the use of camera surveillance. However, since she classified the use of camera surveillance as a "rule and regulation", the arbitrator concluded that s. 4.01 of the collective agreement permitted her to assume jurisdiction over the dispute.

2. Is it obligatory for the employer to define the purpose of the use of camera surveillance? Is this bound to certain purposes (for instance security and safety, the protection of the property of the enterprise, the control of production process, the control of the performance of the worker….). Is it allowed to use camera surveillance for the surveillance of a certain employee or certain employees at the workplace? Is camera surveillance allowed in toilets, dressing rooms or staff rooms?

Short answer: *Under PIPEDA, employers are obligated to define their purpose(s) for using camera surveillance. This is clearly articulated in Principle 4.2 of PIPEDA. While PIPEDA does not enumerate a list of legitimate purposes, the statute does limit the purposes to those that a reasonable person would consider appropriate in the circumstances (s. 5(3)). As well, there is no explicit prohibition against using cameras to monitor certain employees in the workplace. The question is one of balancing the privacy interests of employees, and business interests of employers (s. 3). The same balancing occurs when cameras are placed in highly intrusive locations – such as washrooms or dressing rooms. The general approach is: the more intrusive the surveillance, the higher the onus on employers to justify camera use.*

Is it obligatory for the employer to define the purpose of the use of camera surveillance? Is this bound to certain purposes (for instance security and safety, the protection of the property of the enterprise, the control of production process, the control of the performance of the worker…)?

Principle 4.2 of *PIPEDA*'s Schedule stipulates that employers must identify, to their employees, or an individual employee, the purpose(s) behind surveillance camera use. This must be done at or before the time of information collection (McNairn, above, p. 38). This principle is further expanded in the Schedule (*PIPEDA*, Principles 4.2.1-4.2.6; McNairn, above, p. 38; paraphrased):

- employers shall document the purposes for which personal information is collected;
- identification of purposes at or before the collection allows employers to determine the information needed to fulfil the purposes;
- identification of purposes may be done orally or in writing, depending on the circumstances;
- when personal information is collected and used for a purpose not previously identified, the new purposes shall be identified prior to the use;
- persons authorized to collect information should be able to explain to employees the purposes for which the information is collected;
- the identified purposes serve as a limitation on the scope of information that an employer may collect from an individual employee, or employees;

- employers must limit the amount and type of information collected to what is necessary to fulfil the identified purposes (see *PIPEDA*, clause 4.4.1).

Provisions in *PIPEDA* are general in nature, and apply to different forms of information collection through different media. Thus, there are no specified purposes for the use of camera surveillance. However, jurisprudence and s. 5(3) limit purposes to those that only a reasonable person would consider appropriate in the circumstances (McNairn, above, p. 39; *Eastmond*, above; *Wansink v. Telus Communications Inc.*, 2007 FCA 21, [2007] 4 F.C.R. 368 (*Wansink*)). As already elaborated above (see Question 1), the reasonable purpose test is one that balances interests of privacy (employees) and organizational need (employers). Four contextual factors must be examined in relation to camera use: a) its necessity; b) its effectiveness; c) the proportionality of privacy lost to the employee against the benefit gained to the employer; and d) the existence of a less-invasive way to achieve the same end (*Eastmond*, above, at paras. 126-127; see also Question 1, p. 4 of this document).

In *Eastmond*, the explicit purpose of camera surveillance was to protect the company against theft, vandalism, and related incidents. The employer argued that video surveillance would not be used to monitor productivity issues (*Eastmond*, above, at para. 5). The Court found this purpose to be reasonable because: a) there were legitimate security concerns on the part of the employer, supported by past incidents of vandalism, sexual harassment, and theft; b) videotaping and warning signs were effective to deter further incidents; c) the collection was not surreptitious or continuous, there was a low expectation of privacy since cameras were in public areas, and recordings were kept under lock and key – accessible only by responsible managers and railway police; d) the employer examined alternatives that were neither cost effective or would be disruptive to the employer's operations (*Eastmond*, above, at paras. 174-182; McNairn, above, p. 40).

In another case (*PIPEDA* Case #2004-269), a company hired a private investigator to capture (on video) an employee's activities outside of work. After years of difficulty in obtaining medical information from the employee, the company became increasingly suspicious of the employee's claims for medical accommodation. The purpose of the surveillance was to determine whether the employee was violating his employment contract by misrepresenting the state of his health. The Assistant Privacy Commissioner was satisfied, after applying the four-part analysis, that the purpose was reasonable. The Assistant Privacy Commissioner stated that the purpose was based on substantial evidence that the relationship of trust had been broken. Furthermore, the company had tried (to no avail) less privacy-invasive ways to gather information (http://www.priv.gc.ca/cf-dc/2004/cf-dc_040423_e.cfm).

Labour arbitrators use similar factors to balance privacy against business interests of workers and employers, respectively (McNairn, above, p. 39; see also *Ross v. Rosedale Transport Ltd.*, [2003] C.L.A.D. No. 237; and *Fraser Surrey Docks Ltd. v. International Longshore Warehouse Union Ship and Dock Foremen, Local 514*, [2007] C.L.A.D. No. 48). According to the Federal Court in *Eastmond* (above), arbitrators generally condemn the use of cameras to record the productivity of workers, especially if done surreptitiously (at paras. 132-133).

Is it allowed to use camera surveillance for the surveillance of a certain employee or certain employees at the workplace?

There is no explicit bar against using cameras in the workplace. The question is always one of balancing the privacy of individuals against business interests (s. 3). However, as previously stated, arbitrators, the Privacy Commissioner and the Courts generally denounce the use of surveillance cameras to monitor employee performance. In general, they stipulate camera use as a last resort. The cases that follow illustrate the treatment of camera surveillance in the workplace. As exemplified below, adjudicators have contemplated or applied principles of the reasonable purpose test.

a) ***Re Puretex Knitting Co. Ltd. and Canadian Textile and Chemical Union*** **(1979), 23 L.A.C. (2d) 14 (as cited in *Eastmond,* above, at paras. 135-143):** The purpose of nine cameras in the company was to deter theft. They were not hidden, or designed to aptly supervise employee performance. However, the arbitrator ruled that the cameras in the production areas of the plant was not justifiable or reasonable. Even if these cameras were rotating and incapable of constant surveillance on employees, their presence was "objectionable because the employees experience a sense of constant surveillance since they cannot keep track of the camera's movements" (see *Eastmond,* above, at para. 142). The arbitrator concluded that "any use of cameras that observe employees at work is intrinsically seriously objectionable in human terms, with the degree of objection depending on the way the cameras are deployed and the purpose for which they are used (as cited in *Eastmond*, above, at para. 141).

b) ***Ross v. Rosedale Transport Ltd.*****, [2003] C.L.A.D. No. 237 (as cited in *Eastmond,* above, at paras. 144-152):** An employee was the subject of surreptitious video surveillance by private detectives hired by his employer. The company suspected the employee had been defrauding it deliberately by not returning to work after a work-related back injury. The video had caught the individual lifting and carrying furniture from a house to a pick-up truck. The arbitrator determined that the surveillance evidence would be excluded. There was no evidence that the employee had been dishonest, or had a disciplinary record. It was open to the company to ask for independent medical examination, rather than resort to surreptitious surveillance. According to the arbitrator (as cited in *Eastmond*, above, at para. 151):

> As a general rule, it [the employer's interest] does not justify resort to random videotape surveillance in the form of an electronic web, cast like a net, to see what it might catch. Surveillance is an extraordinary step which can only be resorted to where there is, beforehand, reasonable and probable cause to justify it.

c) ***PIPEDA*** **Case #2004-265 (http://www.priv.gc.ca/cf-dc/2004/cf-dc_040219_02_e.cfm)**: In this case, the usual purpose for the cameras was to monitor train movements, to inform crew members of train locations, and enhance workplace safety. However, the employer began using the cameras to monitor two employees who were suspected of leaving company property during regular work hours. The Assistant Privacy Commissioner found

this latter purpose unreasonable because the employer had no evidence that unauthorized absences were a persistent problem; nor was there any evidence that the employer tried less intrusive efforts to manage the problem of unauthorized absences. According to the Assistant Privacy Commissioner, using video surveillance, "to monitor employee productivity or to manage the employer/employee relationship will, have a chilling effect on employee morale, if it goes unchecked".

d) ***PIPEDA* Case #2005-290 (http://www.priv.gc.ca/cf-dc/2005/290_050127_e.cfm):** A food inspector with the Canadian Food Inspection Agency was inspecting a registered meat processing plant (meat company). The meat company had 15 cameras set up in the plant, including the evisceration room where the food inspectors had their work stations. According to the meat company, the cameras were used to address security concerns, monitor hygiene and safety, ensure food safety, and allow the plant manager to respond quickly to interruptions in the production line. Evidence showed that footage from the evisceration room was sent to the Canadian Food Inspection Agency, in an attempt to undermine the work of the food inspectors. The Assistant Privacy Commissioner found that the purpose of the cameras in the evisceration room was not reasonable. First, their positioning in the evisceration room was not useful to monitor safety, or productivity in the plant. Further, there was a "clear loss of privacy" for the food inspectors. The Assistant Privacy Commissioner recommended that the meat company stop camera surveillance in the evisceration room.

e) ***PIPEDA* Case #2009-001(http://www.priv.gc.ca/cf-dc/2009/2009_001_0219_e.cfm):** An employee complained that his employer, an inter-city bus company, was using 22 video cameras to monitor and manage employee performance. The company provided three specific purposes for the collection and use of information by video surveillance: 1) ensure safety and security of customers and employees against violent criminal activity; 2) reduce and discourage incidents of vandalism and illegal conduct; and 3) limit the potential for liability of damages due to fraud, theft or inappropriate operational procedures. The Assistant Privacy Commissioner determined that the stated purposes were well-supported by evidence of criminal activity, and were an effective means to fulfill the company's needs. The Assistant Privacy Commissioner was also satisfied that the company was not using cameras to monitor work performance. As such, the use of cameras and their purposes were reasonable. According to the Assistant Privacy Commissioner, there was no doubt that the cameras would inadvertently collect employee information. However, if the employer later wished to use the footage for workforce management purposes, s. 7(2)(a) and (b) of *PIPEDA* must be satisfied. Namely, (a) the employer would need to have reasonable grounds to believe the information could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction; or (b) the footage would be "used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual".

Is camera surveillance allowed in toilets, dressing rooms or staff rooms?

With respect to washroom surveillance or other highly intrusive forms of surveillance, one must remember that *PIPEDA* protects privacy interests, but does not make them absolute. As such, the more intrusive the surveillance, the more serious and substantiated the purpose must be. There is no provision directly addressing the use of camera surveillance in washrooms. However, decisions from the Courts, labour arbitrators and the Privacy Commissioner have touched on the issue.

Very few cases from Canadian Courts have dealt with video surveillance in washrooms at the workplace. However, electronic surveillance has been considered in criminal cases within the context of unreasonable search and seizure under s. 8 of the *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11 (*Charter*). In *R. v. Silva* (1995), 26 O.R. (3d) 554, [1995] O.J. (3d) 3840 (QL) (*Silva*) (Ont. Gen. Div.), police installed surreptitious surveillance cameras in public washroom stalls to videotape illegal homosexual activity. The trial judge found this to breach s. 8 of the *Charter* and excluded the evidence; the crown appealed this decision to the General Division. Justice Zelinski of the General Division dismissed the appeal and also found the video surveillance a breach of s. 8 (*Silva*, above, at para. 50). In coming to this conclusion, Justice Zelinski examined relevant jurisprudence from the Supreme Court of Canada (see *R. v. Duarte* (1990), 53 C.C.C. (3d) 1; *R. v. Wong* (1990), 60 C.C.C. (3d) 460). According to the Supreme Court in *Wong* (as cited in para. 44 of *Silva*):

> [U]nauthorized surreptitious electronic surveillance may, in certain circumstances, violate an individual's rights under s. 8. I agree that such surveillance will violate s. 8 where the target of the surveillance has a reasonable expectation of privacy. However, in my view, the consideration of whether an individual has a reasonable expectation of privacy can only be decided within the particular factual context of the surveillance, not by reference to a general notion of privacy in a free and democratic society which an individual enjoys at all times. A person has the right under s. 8 to be free from unauthorized surreptitious electronic surveillance where that person has a reasonable expectation that the agents of the state will not be watching or recording private activity nor monitoring or recording private conversations. [Emphasis added.]

In line with this, Justice Zelinski determined (*Silva*, above, at para. 45):

> It would be difficult, in my view, to find many ‘public’ places where there is more ‘reason’ for an ‘expectation of privacy’ than in the closed cubicle of a public washroom.

There is no doubt that the criminal and employment contexts are different. This can be gleaned from the Ontario Labour Arbitration decision, *Cargill Foods, a Division of Cargill Ltd. v. United Food and Commercial Workers International Union, Local 633 (Privacy Grievance)*, [2008] O.L.A.A. No. 393, 175 L.A.C. (4th) 213 (*Cargill*). The arbitrator observed (*Cargill*, above, at para. 83):

> It is fair to say that employees in all industrial plant do not have a reasonable expectation of privacy, in this sense of freedom from observation, while they are performing work and subject to supervision. If they were so entitled, there, could be no direct supervision.

Given the above, it cannot be said that employees are totally devoid of privacy rights. While privacy interests may not be engaged by the mere fact of being under observation, it is clear that "some intrusive forms of observation might be so unwelcome as to amount to harassment, thereby engaging the privacy interest" (*Cargill*, above, at para. 84). It could be argued that video surveillance of washroom use, or cameras in the washroom constitute such intrusive forms of observation.

The same theme extended to the Canadian Labour Arbitration decision, *Cascade Aerospace, Inc. v. National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada), Local 114 (Surveillance Group/Policy Grievance)*, [2009] C.L.A.D. No. 95, 186 L.A.C. (4th) 26 at paragraph 78 (*Cascade Aerospace*). According to the arbitrator, past arbitral decisions were clear that:

> Although privacy rights are not absolute, employees are entitled to expect privacy in certain contexts, e.g. while having their lunch, or going to the washroom; and, video surveillance is not acceptable as an ordinary method for supervising employees at their work. The need for surveillance must be reasonable and sensitive to the balance of interests of the employer and the persons affected. [Emphasis added.]

In 2007, the Privacy Commissioner's Office dealt with a complaint about non-video surveillance outside a washroom. A log of washroom visits was kept, with the name of the individual noted on a sheet of paper, along with the time the person entered the facility. According to the Assistant Privacy Commissioner, a log of washroom visits was privacy invasive. Physical surveillance of individuals in the washroom would have been "highly privacy invasive" (*PIPEDA* Case #2007-379, http://www.priv.gc.ca/cf-dc/2007/379_20070404_e.cfm). In applying the four-part test of s. 5(3) of *PIPEDA*, the Assistant Privacy Commissioner determined the surveillance and its purpose to be unreasonable.

The sum of these decisions illustrate that generally video surveillance (especially surreptitious) of employees in washrooms or dressing rooms, is an extreme intrusion of privacy. Thus, where employers seek to engage in this type of surveillance, they likely need to show serious interests at stake to counterbalance the extreme invasion of privacy.

3. To whom are the sequences available?

Short answer: *Footage from surveillance cameras can be accessed by employers and designated staff, as well as by individual employees captured on film. Access by employers, managers or security personnel is governed by Principles 4.1 and 4.7 of the Schedule. On the other hand, ss. 8 and 9 of PIPEDA and Principle 4.9 outline the scope of access by individual employees.*

PIPEDA does not contain any explicit provision outlining who in the organization can access the surveillance footage. According to Principle 4.1 (Accountability), an organization (or employer) is responsible for the personal information under its control, and it shall designate specific individual(s) to make sure the organization complies with *PIPEDA* and the Schedule. Under this broad umbrella of accountability, an employer must create and implement policies and practices regarding the maintenance of this information. Where a complaint is filed, the Privacy Commissioner can enforce this principle and make relevant recommendations. This was seen in *PIPEDA* Case #2009-001 (above). The Assistant Privacy Commissioner made the following recommendations to the employer:

a) Finalize its video surveillance policy, and specify that access to footage can only be granted to security personnel and managers after less intrusive methods have been tried unsuccessfully.

b) Finalize specific procedures for security personnel and managers regarding access to videotapes where the need arises in relation to the purposes identified by the employer.

c) Train security personnel and managers on procedures for accessing videotapes to fulfil purposes identified by the employer.

Principle 4.7 deals with safeguards: “personal information shall be protected by security safeguards appropriate to the sensitivity of the information”. Pursuant to Principle 4.7, the Schedule enumerates the following guidelines:

a) Security safeguards shall protect personal information against loss, theft, unauthorized access, disclosure, copying, use or modification (*PIPEDA*, Principle 4.7.1).

b) The nature of the safeguards will vary according to the sensitivity of the information, the amount, distribution and format of the information. The more sensitive the information, the higher the level of protection (*PIPEDA*, Principle 4.7.2).

c) The methods of protection should include: physical measure (locks, restricted office access); organizational measures (security clearance); and technological measures (passwords or encryption) (*PIPEDA*, Principle 4.7.3).

d) Organizations shall make their employees aware of the importance of maintaining confidentiality with respect to personal information (*PIPEDA*, Principle 4.7.4).

Adjudicators have looked favourably on appropriate safeguarding of surveillance footage. The Federal Court in *Eastmond* (above) found that the employer kept recorded images under lock and key, and made sure recordings were only accessible to responsible managers and police if an incident was reported (at para. 176). The Federal Court considered this factor in its s. 5(3) analysis, and concluded that the use of video surveillance was reasonable and minimally impairing on privacy interests of employees.

Second, surveillance footage can be accessed by the individual employee who was caught on tape. The scope and limits of this access are stipulated in ss. 8 and 9 of *PIPEDA* and Principle 4.9 (Individual Access) of the Schedule. Under Principle 4.9, upon request, the individual employee or employees shall be informed of the existence, use and disclosure of his or her personal information, and shall be given access to that information (see also Principle 4.9.1). This way, the individual has the ability to challenge the accuracy and completeness of the information. For the full text of Principle 4.9, please see **Appendix A**.

Section 8 of *PIPEDA* sets out the procedures for individuals to access video footage. According to s. 8(1), a request for access must be made in writing. The organization is mandated to respond to a request with due diligence and within 30 days after receipt of the request (s. 8(3)). If the organization does not respond within the time limit, the employer is deemed to have refused the request (s. 8(5)). Costs can be imposed on the individual, but only if the organization has informed the individual of the costs, and the individual has advised the organization that the request is not being withdrawn (s. 8(6)). Written reasons are required if the organization responds within the time limit and refuses the request (s. 8(7)).

Pursuant to s. 9(1) of *PIPEDA*, individual access can be prohibited if it will reveal personal information about a third party. However, if the information concerning a third party is severable, it must be severed before giving the individual access.

4. <u>How long are they stored?</u>

Short answer: *There is no explicit limit on how long camera surveillance must be stored. Length of storage is based on the circumstances of each case. Principles 4.5 and s. 8(8) of PIPEDA set out potential maximum or minimum time frames for storage.*

Principle 4.5 of the Schedule deals with retention of the personal information, in this case, surveillance footage. According to Principle 4.5, footage shall be retained only as long as necessary for employers to fulfil their stated purposes. Furthermore, organizations should develop guidelines and implement procedures with respect to the retention of personal information (*PIPEDA*, Principle 4.5.2). Such guidelines should include minimum and maximum retention periods; however, personal information that was used to make a decision about an individual should be retained long enough to allow individual access after decision has been made (*PIPEDA*, Principle 4.5.2). If personal information is no longer required to fulfil the

identified purposes, it should be destroyed, erased, or made anonymous. Organizations should develop guidelines and procedures for the destruction of personal information (*PIPEDA*, Principle 4.5.3).

Provisions of *PIPEDA* slightly modify Principle 4.5. The statute establishes a maximum retention period under s. 8(8):

> Despite clause 4.5 of Schedule 1, an organization that has personal information that is the subject of a request shall retain the information for as long as is necessary to allow the individual to exhaust any recourse under this Part that they may have.

While this provision could to impose a serious burden on the employer, one must remember that the purpose of *PIPEDA* is to balance interests of employers and employees. The Federal Court applied this balancing principle to the interpretation of s. 8(8) in *Johnson v. Bell Canada*, 2008 FC 1086, [2009] 3 F.C.R. 67, 334 F.T.R. 44. According to Justice Zinn (*Johnson*, above, at para. 52; see also McNairn, above, p. 75):

> It is impractical to require a company like Bell Canada to stop its corporate retention policies each time an access request is made; especially as it is not known if any of the information that would otherwise be lost into the abyss is even responsive to the request. From a practical and pragmatic standpoint, what subsection 8(8) of PIPEDA requires of an organization is that it retain that information that it has discovered in its search that is or may be responsive to the request, until the person making the request has exhausted all avenues of appeal.

5. Is there an obligation to inform employees if camera surveillance is installed? Does the use of camera surveillance require the consent of the employees?

Short answer: *There is a general obligation on employers to obtain knowledge and consent before of employees before collecting personal information. However, consent, whether explicit or implicit, can be waived in a variety of circumstances under s. 7 of PIPEDA. Due to the controversy surrounding covert camera surveillance, the Privacy Commissioner's Office has created a Guidance Document for employers to follow.*

Under *PIPEDA*, if an employer wants to have camera surveillance installed, it must *prima facie* ensure its employees have knowledge and are aware of the situation (McNairn, above, p. 41). This obligation is found under Principle 4.3 of *PIPEDA*'s Schedule. Knowledge and consent has been interpreted to mean "informed consent" (McNairn, above, p. 56). McNairn provides an example of adequate informed consent (above, p. 56; see also *Wansink*, above, at para. 32):

> If an employer asks an employee to consent to the collection, use or disclosure of his or her personal information and a refusal to

> consent could lead to disciplinary action against the employee, such as suspension or firing, the employer must disclose those potential consequences up front for any resulting consent to be informed.

Consent not only applies to collection, but also the use of surveillance footage. Under Principle 4.3.2, an employer is mandated to make reasonable efforts to ensure that the employee is advised of the purposes for which the information is to be used. Furthermore, "to make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used and disclosed" (*PIPEDA*, Principle 4.3.2; see also McNairn, above, p. 56-57).

Depending on the circumstances and the sensitivity attached to the information, consent can be sought in a variety of ways. Where information is likely considered sensitive (such as health), express consent should be sought. On the other hand, implied consent would be appropriate with less sensitive information or where cameras are located in public places. As such, reasonable expectations of individuals, with regard to the particular information and location of the camera, are relevant (see *PIPEDA*, Principles 4.3.4, 4.3.5, 4.3.6; McNairn, above, p. 58-59). The Privacy Commissioner's Office has previously examined the issue of "implied consent". In *PIPEDA* Case #2009-001 (above), the Assistant Privacy Commissioner held that consent is assumed when:

a) information collected is not sensitive; and

b) the express purposes of the video surveillance have been explained so that the employees would reasonably expect that their information is used only for those purposes.

Implied consent to videotaping may arise when an individual enters onto property that has signs clearly indicating the presence of camera surveillance. However, some contend that the situation is different in the employment context. No implied consent is likely to arise if the individual being taped is an employee, and the location is his or her place of work. "Indeed, in any situation where the individual does not have a free choice as to whether to enter the property, there will be no reasonable basis for implying consent" (McNairn, above, p. 59).

While there is a strong push for employers to seek consent, this requirement is not absolute. Provisions in *PIPEDA* and Principle 4.3 contemplate situations where covert surveillance may be allowed. According to the Note in Principle 4.3, in certain circumstances personal information can be collected, used or disclosed without knowledge or consent, for example:

a) legal, medical or security reasons may make seeking consent impractical or impossible.

b) when information is being collected to detect or prevent fraud or crime, seeking consent would undermine or defeat the purpose of using camera surveillance.

Section 7(1) of *PIPEDA* expands on Principle 4.3, and provides circumstances when covert surveillance is allowed. Under s. 7(1), employers may not need to obtain consent when:

a) the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;

b) 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 […]

According to McNairn, employers who collect personal information on employees through video surveillance usually do it "for the purpose of investigating either a breach of an agreement, namely an employment or collective agreement... or, if the surveillance is for security reasons, a contravention of the law by one or more employees or others" (above, p. 43). In order to rely on the investigation exception, under s. 7(1)(b), an organization must be able to show that knowledge or consent of the affected individual would adversely affect the availability or accuracy of the information (see McNairn, above, p. 44; *Eastmond*, above, 189).

The Privacy Commissioner examined the issue of covert surveillance in *PIPEDA* Case #2007-379 (above) and set out the following test to satisfy s. 7(1) of *PIPEDA*:

a) the collection of personal information must be only for purposes that a reasonable person would consider appropriate in the circumstances.

b) there must be substantial evidence to support the suspicion that a relationship of trust has been broken or a law contravened.

c) the organization must have exhausted all other means of collecting the information in less privacy-invasive ways.

d) the collection must be limited to the purposes as much as possible.

Subsequent to the decision above, on May 27, 2009, the Privacy Commissioner issued a Guidance Document titled: "*Guidance on Covert Video Surveillance in the Private Sector*" (see http://www.priv.gc.ca/information/pub/gd_cvs_20090527_e.cfm). This Guidance Document elaborates on the four-part test in *PIPEDA* Case #2007-379 (above). (Please see **Appendix B** for the full document.)

First, on the question of purpose, the Guidance Document reiterates the reasonableness test found under s. 5(3) of *PIPEDA* and endorsed by the Federal Court in *Eastmond* (above; see also Question #1 of this memorandum). Second, on "substantial evidence" to engage covert surveillance, the Guidance Document states that employers "cannot simply rely on mere suspicion but must in fact have evidentiary justification". Finally, on limiting collection, the Privacy Commissioner's Office recommends that the use of covert surveillance should be limited to both the type and amount of information that is necessary to fulfill the identified purpose.

Employers need to be very specific about the kind of personal information they are looking to collect, and should limit the duration and scope of the surveillance. Furthermore, the surveillance should be conducted in a fair and lawful manner.

The Guidance Document also outlines the type of policies that employers should implement for covert video surveillance, and best practices for employers who choose to use private investigation firms to perform covert video surveillance.

6. Is there an obligation to inform the works council or trade unions about the introduction and the use of camera surveillance? Is there an obligation to have an agreement with the works council or trade unions defining the circumstances and conditions for the introduction and use of camera surveillance?

Short answer: *The obligation to inform trade unions is based mainly on two things: terms in the collective agreement, and general principles in PIPEDA and the Schedule. Much like consent with respect to individuals, the question is one of balancing interests.*

An employer's obligation to inform or consult trade unions on camera use generally arises from terms of the collective agreement. As seen in the answer to Question #1 of this memorandum, some collective agreements are explicit on camera use, while others are silent. Where terms are silent on camera surveillance, labour arbitrators have examined provisions related to management rights. Often, these rights include ancillary obligations on employers to ensure union representatives are informed when new rules or regulations are implemented. In interpreting these broad management rights and obligations, labour arbitrators have recognized the importance of protecting employees' privacy interests. To do so, it is vital to keep union representatives informed. According to *Cascade Aerospace*, collective agreements often bestow upon unions exclusive power to bargain on behalf of individual employees (above, at para. 39).

Labour arbitrators have applied *PIPEDA*'s principles of reasonable purpose and consent to labour disputes. This has occurred even when employers involved in the grievance were not federal works, undertakings or businesses (see *Janes Family Foods*, above, p. 13). Where a collective agreement is silent on camera surveillance and union representatives have not been notified on actual camera use, the following questions have been considered by labour arbitrators in Canada: a) is camera use a "rule or regulation"; b) if so, is this rule or regulation reasonable; and c) is notice to the Union required?

With respect to the first question, arbitrators have found that surveillance camera use can constitute a "rule" or "regulation". According to *Janes Family Foods*, above, "rules and regulations" are employer actions that impact on the employees personally (above, p. 10). Camera use is characterized as a rule or regulation because it regulates the individual conduct of each employee – workers have no option but to comply (*Janes Family Foods*, above, p. 10). Consequently, where camera use has been interpreted as a rule or regulation in a particular case, collective agreements generally require employers to inform union representatives before the

installation and operation of surveillance cameras (see *Janes Family Foods*, above; *Cascade Aerospace*, above; *Cargill*, above).

Under the second question, collective agreements often mandate that rules and regulations be reasonable (see *Janes Family Foods*, above; *Cascade Aerospace*, above). Labour arbitrators often lift the test and principles of reasonableness from *PIPEDA*. In *Cascade Aerospace* (above), a Canadian Labour arbitrator found that the company installed a hidden surveillance camera in the cafeteria, and did not inform the Union. The company argued the camera was used to investigate incidents of vandalism on a vending machine. According to the Union, this was a violation of the collective agreement, and principles in *PIPEDA.* The camera not only captured images around the vending machine, but also tables where Union members met and held ballots. In determining whether the purpose of the hidden camera was reasonable, the arbitrator cited the four-part test in *Eastmond* (above; see also *Cascade Aerospace*, above, at paras. 78-87). The arbitrator found that the company has justified in using the hidden camera to investigate vandalism. However, it was not reasonable to extend the range of surveillance beyond the vending machine to areas where union members met (*Cascade Aerospace*, above, at para. 87).

In considering the third question of notice, one must determine whether the surveillance at issue is covert or overt. The arbitrator in *Cascade Aerospace* turned to s. 7(1)(b) of *PIPEDA* in instances of covert surveillance. Under s. 7(1)(b) no knowledge and consent is required from where "it is reasonable to expect that the collection with knowledge or consent…would comprise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating" breaches of agreement, or contraventions of Canadian or provincial laws (see *Cascade Aerospace*, above, at para. 81).

Where surveillance is overt and cameras are clearly visible, the arbitrator in *Cascade Aerospace* held that the union had an obligation to raise the issue during collective bargaining (above, at para. 95):

> If the lack of formal notice is a problem, that now cannot be taken as a serious complaint when the Union's collective bargaining committee did not ask one question about cameras in the collective bargaining that was going on at the time. This is not to say that the Union has waived its rights; but, that the notice question is severable, and, that it is now moot and not material to the substance of the dispute.

From the sampling of cases above, no strict rule forces employers to inform union representatives on camera use. Rather, the need to inform is highly dependent on the collective agreement, and circumstances of the particular case. As well, there is no statutory obligation to include provisions on camera use in collective agreements.

7. Has the employer (controller, who uses electronic technology to process personal data) the duty to notify the processing to the Data Protection Authority or another authority? Do employers need a permit from the Authority before he can set up the camera? What are the conditions for the Permission for camera surveillance? Has the Data Protection Authority the authority to impose changes in order to make the processing or the surveillance satisfy the requirements of the law?

Short answer: *There is no explicit legal duty for employers to notify the Privacy Commissioner's Office before camera surveillance is installed and used. However, the Privacy Commissioner can initiate or receive complaints regarding an employer's potential violation of PIPEDA. The Privacy Commissioner has the power to make recommendations and monitor an employer's compliance with these recommendations. If unsatisfied with the result of a complaint, the employee(s) can make an application to the Federal Court.*

Has the employer (controller, who uses electronic technology to process personal data) the duty to notify the processing to the Data Protection Authority or another authority? Do employers need a permit from the Authority before he can set up the camera? What are the conditions for the Permission for camera surveillance?

There is no explicit duty on employers to notify the Privacy Commissioner's Office on camera use – whether overt or covert.

According to *PIPEDA* Case #2004-265 (above), the Privacy Commissioner's Office has a lead role is "in determining whether organizations subject to the Act are adhering to it, and in educating them about their obligations, and the public about its rights, under the Act." Pursuant to s. 18 of *PIPEDA*, the Privacy Commissioner may, on reasonable notice at any reasonable time, audit the personal information management practices of an organization. This may be done if the Privacy Commissioner has reasonable grounds to believe that provisions of *PIPEDA* are being contravened. There is also a complaint system in place. Under s. 11(1) of *PIPEDA*, an individual may file a written complaint against their employer for contravening provisions in the legislation, or for not following a recommendation set out in the Schedule. The Privacy Commissioner may also initiate a complaint if he or she is "satisfied that there are reasonable grounds to investigate" an organization or employer (s. 11(2)).

Once a complaint is launched, the Commissioner, pursuant to s. 12 of *PIPEDA*, has the power to investigate and attempt to resolve complaints by means of dispute resolutions, such as mediation or conciliation. Within a year after a complaint is filed, or initiated, the Commissioner must prepare a report of his or her findings, and relevant settlements (s. 13). If unsatisfied, the complainant may apply to the Federal Court (s. 14). A proceeding under s. 14 of *PIPEDA* is not a judicial review, but a "fresh application" in order to obtain a remedy under s. 16 (*Eastmond*, above, at para. 118). There is no deference to the Privacy Commissioner's decision if additional evidence is presented. According to Justice Lemieux in *Eastmond*, "the situation before me [is] analogous to proceedings under the Trade Marks Act" (above, at para. 124). See also McNairn, above, pages 86-87; *Englander v. Telus Communications Inc.*, 2004 FCA 387, [2005] 2 F.C.R.

572. The burden rests with the applicant to show that the employer violated its *PIPEDA* obligations (*Eastmond*, above, at para. 118).

Has the Data Protection Authority the authority to impose changes in order to make the processing or the surveillance satisfy the requirements of the law?

To ensure compliance with *PIPEDA*, the Privacy Commissioner has the power to make recommendations, and ask employers to report back within specified timelines (see *PIPEDA* Case #2009-001, above; *PIPEDA* Case #2007-379, above; *PIPEDA* Case #2005-290, above).

Under s. 16 of *PIPEDA*, the Federal Court has the discretion, in addition to any other remedies it gives, to

a) order an organization to correct its practices in order to comply with sections 5 to 10;

b) order an organization to publish a notice of any action taken or proposed to be taken to correct its practices, whether or not ordered to correct them under paragraph (a); and

c) award damages to the complainant, including damages for any humiliation that the complainant has suffered.

According to the Federal Court of Appeal in *Englander* (above), s. 16 bestows upon the Court "remarkably broad" remedial powers (at para. 47). Based on the language in s. 16, the Court "is not limited in its ability to grant other remedies pursuant to its general jurisdiction, including its inherent jurisdiction as a superior court of record" (McNairn, above, p. 87). This means, for example, that the Federal Court can order an employer to correct its practices to comply with *PIPEDA*, and order it to disclose a complainant's personal information in response to a request for information under s. 11 of *PIPEDA* (see McNairn, above, p. 87).

8. What are the consequences of a failure to comply with the rules on camera surveillance (for instance punishment; liability to pay damages; works council or trade unions or worker can demand the control measures to be stopped and the prior situation to be restored….)?

Apart from the remedial powers listed under Question #7, *PIPEDA* also stipulates penalties for organizations and employers who do not comply with its provisions and principles. Under s. 28 of *PIPEDA*, anyone who obstructs the Privacy Commissioner or the Commissioner's delegate in the investigation of a complaint or in conducting an audit is guilty of an offence. Furthermore, everyone who knowingly destroys personal information that is subject to an access request (s. 8(8)) is also guilty of an offence under *PIPEDA*. If convicted summarily, an employer is liable to a maximum fine of $10,000. For an indictable offence, the maximum fine is $100,000.

III) CONCLUSION

PIPEDA is an important piece of legislation for protecting the privacy interests of employees working in federal works, undertakings, or businesses from excessive camera surveillance by employers. The statute does not impose strict rules on employers. Rather, a more flexible approach exists to balance privacy and business interests.

As discussed in this paper, the Canadian Courts, the Privacy Commissioner and, labour arbitrators have interpreted and applied provisions or principles derived from *PIPEDA*. The statute has also been lauded by scholars, particularly on the "reasonable purpose" test under s. 5(3). According to Austin, from the Faculty of Law at the University of Toronto, the test is well suited to address different concerns and situations (see Austin, above). However, Austin states that this test cannot adequately protect privacy rights unless it includes, as a first step, an inquiry into the nature and scope of those interests at stake. The reasonable purpose test, as it now stands, "looks like a kind of orphaned *Oakes* test from *Charter* jurisprudence – defining when a right might be limited but missing the important initial step of defining the right in question and the manner in which it is being violated" (Austin, above, p. 23 of QL). According to Austin, to enhance *PIPEDA*'s effectiveness, its fair information principles must be examined in light of constitutional law. This is important as Courts have recognized *PIPEDA* as quasi-constitutional.

In improving *PIPEDA*, it is also crucial to look beyond Canada's borders. One must not forget that *PIPEDA* has deep international roots in the *OECD Guidelines*. By comparing *PIPEDA* to other domestic schemes around the world, Canada can better reflect and improve our data protection laws, and ensure our international obligations are being met.

APPENDIX A

SCHEDULE 1
(Section 5)
PRINCIPLES SET OUT IN THE NATIONAL STANDARD OF CANADA ENTITLED MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION, CAN/CSA-Q830-96

4.1 Principle 1 — Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

4.1.1

Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

4.1.2

The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.

4.1.3

An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

4.1.4

Organizations shall implement policies and practices to give effect to the principles, including

(*a*) implementing procedures to protect personal information;

(*b*) establishing procedures to receive and respond to complaints and inquiries;

(*c*) training staff and communicating to staff information about the organization's policies and practices; and

(*d*) developing information to explain the organization's policies and procedures.

4.2 Principle 2 — Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

4.2.1

The organization shall document the purposes for which personal information is collected in order to comply with the Openness principle (Clause 4.8) and the Individual Access principle (Clause 4.9).

4.2.2

Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfil these purposes. The Limiting Collection principle (Clause 4.4) requires an organization to collect only that information necessary for the purposes that have been identified.

4.2.3

The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

4.2.4

When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Clause 4.3).

4.2.5

Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

4.2.6

This principle is linked closely to the Limiting Collection principle (Clause 4.4) and the Limiting Use, Disclosure, and Retention principle (Clause 4.5).

4.3 Principle 3 — Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

4.3.1

Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

4.3.2

The principle requires “knowledge and consent”. Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

4.3.3

An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.

4.3.4

The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

4.3.5

In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

4.3.6

The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

4.3.7

Individuals can give consent in many ways. For example:

(*a*) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;

(*b*) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;

(*c*) consent may be given orally when information is collected over the telephone; or

(*d*) consent may be given at the time that individuals use a product or service.

4.3.8

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

4.4 Principle 4 — Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

4.4.1

Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8).

4.4.2

The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

4.4.3

This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3).

4.5 Principle 5 — Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

4.5.1

Organizations using personal information for a new purpose shall document this purpose (see Clause 4.2.1).

4.5.2

Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

4.5.3

Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

4.5.4

This principle is closely linked to the Consent principle (Clause 4.3), the Identifying Purposes principle (Clause 4.2), and the Individual Access principle (Clause 4.9).

4.6 Principle 6 — Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

4.6.1

The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

4.6.2

An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.

4.6.3

Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

4.7 Principle 7 — Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

4.7.1

The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

4.7.2

The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

4.7.3

The methods of protection should include

(*a*) physical measures, for example, locked filing cabinets and restricted access to offices;

(*b*) organizational measures, for example, security clearances and limiting access on a “need-to-know” basis; and

(*c*) technological measures, for example, the use of passwords and encryption.

4.7.4

Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

4.7.5

Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

4.8 Principle 8 — Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

4.8.1

Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

4.8.2

The information made available shall include

(*a*) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;

(*b*) the means of gaining access to personal information held by the organization;

(*c*) a description of the type of personal information held by the organization, including a general account of its use;

(*d*) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and

(*e*) what personal information is made available to related organizations (e.g., subsidiaries).

4.8.3

An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

4.9 Principle 9 — Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Note: In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

4.9.1

Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

4.9.2

An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

4.9.3

In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.

4.9.4

An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.

4.9.5

When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

4.9.6

When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

4.10 Principle 10 — Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

4.10.1

The individual accountable for an organization's compliance is discussed in Clause 4.1.1.

4.10.2

Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.

4.10.3

Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate.

4.10.4
An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.

APPENDIX B

Guidance on Covert Video Surveillance in the Private Sector
(http://www.priv.gc.ca/information/pub/gd_cvs_20090527_e.cfm)

Introduction and scope

The Office of the Privacy Commissioner considers covert video surveillance to be an extremely privacy-invasive form of technology. The very nature of the medium entails the collection of a great deal of personal information that may be extraneous, or may lead to judgments about the subject that have nothing to do with the purpose for collecting the information in the first place. In the Office's view, covert video surveillance must be considered only in the most limited cases.

This guidance is based on the federal private sector privacy law *The Personal Information Protection and Electronic Documents Act* (PIPEDA), and is intended to outline the privacy obligations and responsibilities of private sector organizations contemplating and engaging in covert video surveillance. We consider video surveillance to be covert when the individual is not made aware of being watched.

This document serves as a companion piece to the following guidelines for video surveillance issued by this office: Guidelines for Overt Video Surveillance in the Private Sector (prepared in collaboration with Alberta and British Columbia) and Guidelines for surveillance of public places by police and law enforcement authorities.

Please note that the following is guidance only. We consider each complaint brought before us on a case-by-case basis.

PIPEDA requirements governing covert video surveillance

PIPEDA governs the collection, use and disclosure of personal information in the course of a commercial activity and in the employment context of federally regulated employers[1]. The capturing of images of identifiable individuals through covert video surveillance is considered to be a collection of personal information. Organizations that are contemplating the use of covert video surveillance should be aware of the criteria they must satisfy in order to collect, use and disclose video surveillance images in compliance with PIPEDA. These criteria are outlined below and address the purpose of the covert video surveillance, consent issues, and the limits placed on collecting personal information through covert video surveillance.

A common misconception is that organizations are released from their privacy obligations if covert video surveillance is conducted in a public place. In fact, under PIPEDA, any collection of personal information taking place in the course of a commercial activity or by an employer subject to PIPEDA, regardless of the location, must conform to the requirements described below.

A. Purpose

The starting point for an organization that is contemplating putting an individual under surveillance without their knowledge is to establish what purpose it aims to achieve.

What is the reason for collecting the individual's personal information through covert video surveillance? Under PIPEDA, an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances (subsection 5(3)).

In deciding whether to use covert video surveillance as a means of collecting personal information, an organization should closely examine the particular circumstances of why, when and where it would collect personal information and what personal information would be collected. There are a number of considerations that factor into determining whether an organization is justified in undertaking covert video surveillance. Given the different contexts in which covert video surveillance may be used, the ways in which the factors apply and are analyzed vary depending on the circumstances.

Demonstrable, evidentiary need

In order for the organization's purpose to be considered appropriate under PIPEDA, there must be a demonstrable, evidentiary need for the collection. In other words, it would not be enough for the organization to be acting on a mere suspicion. The organization must have a strong basis to support the use of covert video surveillance as a means of collecting personal information.

Information collected by surveillance achieves the purpose

The personal information being collected by the organization must be clearly related to a legitimate business purpose and objective. There should also be a strong likelihood that collecting the personal information will help the organization achieve its stated objective. The organization should evaluate the degree to which the personal information being collected through covert video surveillance will be effective in achieving the stated purpose.

Loss of privacy proportional to benefit gained

Another factor to be considered is the balance between the individual's right to privacy and the organization's need to collect, use and disclose personal information. An organization should ask itself if the loss of privacy is proportional to the benefit gained. It may decide that covert video surveillance is the most appropriate method of collecting personal information because it offers the most benefits to the organization. However, these advantages must be weighed against any resulting encroachment on an individual's right to privacy in order for a reasonable person to consider the use of covert surveillance to be appropriate in the circumstances.

Less privacy-invasive measures taken first

Finally, any organization contemplating the use of covert video surveillance should consider other means of collecting the personal information given the inherent intrusiveness of covert video surveillance. The organization needs to examine whether a reasonable person would consider covert video surveillance to be the most appropriate method of collecting personal information under the circumstances, when compared to less privacy-invasive methods.

B. Consent

As a general rule, PIPEDA requires the individual's consent to the collection, use and disclosure of personal information (Principle 4.3). It is possible for covert video surveillance to take place with consent. For example, an individual can be considered to have implicitly consented to the collection of their personal information through video surveillance if that individual has initiated formal legal action against the organization and the organization is collecting the information for the purpose of defending itself against the legal action. It is important to note that implied consent does not authorize unlimited collection of an individual's personal information but limits collection to what is relevant to the merits of the case and the conduct of the defence.

In most cases, however, covert video surveillance takes place without consent. PIPEDA recognizes that there are limited and specific situations where consent is not required (paragraph 7(1)(b)). In order to collect information through video surveillance without the consent of the individual, organizations must be reasonably satisfied that:

- collection with the knowledge and consent of the individual would compromise the availability or 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.

The exception to the requirement for knowledge and consent could, in certain circumstances, provide for the collection of a third party's personal information.

In the employment context, an organization should have evidence that the relationship of trust has been broken before conducting covert video surveillance. Organizations cannot simply rely on mere suspicion but must in fact have evidentiary justification.

Regardless of whether or not consent is obtained, organizations must have a reasonable purpose for collecting the information.

C. Limiting collection

When collecting personal information, organizations must take care to limit both the type and amount of information to that which is necessary to fulfill the identified purposes (Principle 4.4). Organizations should be very specific about what kind of personal information they are looking to collect and they should limit the duration and scope of the

surveillance to what would be reasonable to meet their purpose. Moreover, the collection must be conducted in a fair and lawful manner.

As well, organizations must limit the collection of images of parties who are not the subject of an investigation. There may be situations in which the collection of personal information of a third party[2] via covert video surveillance could be considered acceptable provided the organization has reason to believe that the collection of information about the third party is relevant to the purpose for the collection of information about the subject. However, in determining what is reasonable, the organization must distinguish between persons who it believes are relevant to the purposes of the surveillance of the subject and persons who are merely found in the company of the subject. In our view, PIPEDA does not allow for the collection of the personal information of the latter group without their knowledge or consent.

Organizations can avoid capturing individuals who are not linked to the purpose of the investigation by being more selective during video surveillance. If such personal information is captured, it should be deleted or depersonalized as soon as is practicable. This refers not only to images of the individuals themselves, but also to any information that could serve to identify them, such as street numbers and licence plates. We advocate the use of blurring technology when required. Though we acknowledge its cost to organizations, we view the expenditure as necessary given that, pursuant to PIPEDA, the personal information of any individual can only be collected, used and disclosed without consent in very limited and specific situations.

The need to document

Proper documentation by organizations is essential to ensuring that privacy obligations are respected and to protect the organization in the event of a privacy complaint. Organizations should have in place a general policy that guides them in the decision-making process and in carrying out covert video surveillance in the most privacy-sensitive way possible. There should also be a documented record of every decision to undertake video surveillance as well as a record of its progress and outcome.

i. **Policy on covert video surveillance**

Organizations using covert video surveillance should implement a policy that:

- sets out privacy-specific criteria that must be met before covert video surveillance is undertaken;
- requires that the decision be documented, including rationale and purpose;
- requires that authorization for undertaking video surveillance be given at an appropriate level of the organization;
- limits the collection of personal information to that which is necessary to achieve the stated purpose;
- limits the use of the surveillance to its stated purpose;

- requires that the surveillance be stored in a secure manner;
- designates the persons in the organization authorized to view the surveillance;
- sets out procedures for dealing with third party information;
- sets out a retention period for the surveillance; and
- sets out procedures for the secure disposal of images.

ii. **Documenting specific instances of video surveillance**

There should be a detailed account of how the requirements of the organization's policy on video surveillance have been satisfied, including:

- a description of alternative measures undertaken and their result;
- a description of the kind of information collected through the surveillance;
- the duration of surveillance;
- names of individuals who viewed the surveillance;
- what the surveillance was used for;
- when and how images were disposed of; and
- a service agreement with any third party hired to conduct the surveillance, if applicable.

Best practices for using private investigation firms

Many organizations hire private investigation firms to conduct covert video surveillance on their behalf. It is the responsibility of both the hiring organization and the private investigation firm to ensure that all collection, use and disclosure of personal information is done in accordance with privacy legislation. We strongly encourage the parties to enter into a service agreement that incorporates the following:

- confirmation that the private investigation firm constitutes an "investigative body" as described in PIPEDA "Regulations Specifying Investigative Bodies";
- an acknowledgement by the hiring organization that it has authority under PIPEDA to collect from and disclose to the private investigation firm the personal information of the individual under investigation;
- a clear description of the purpose of the surveillance and the type of personal information the hiring organization is requesting;

- the requirement that the collection of personal information be limited to the purpose of the surveillance;

- the requirement that the collection of third party information be avoided unless the collection of information about the third party is relevant to the purpose for collecting information about the subject;

- a statement that any unnecessary personal information of third parties collected during the surveillance should not be used or disclosed and that it should be deleted or depersonalized as soon as is practicable;

- confirmation by the private investigation firm that it will collect personal information in a manner consistent with all applicable legislation, including PIPEDA;

- confirmation that the private investigation firm provides adequate training to its investigators on the obligation to protect individuals' privacy rights and the appropriate use of the technical equipment used in surveillance;

- the requirement that the personal information collected through surveillance is appropriately safeguarded by both the hiring organization and the private investigation firm;

- the requirement that all instructions from the hiring company be documented;

- a provision prohibiting the use of a subcontractor unless previously agreed to in writing, and unless the subcontractor agrees to all service agreement requirements;

- a designated retention period and secure destruction instructions for the personal information;

- a provision allowing the hiring company to conduct an audit.

[1] For information on whether your organization is subject to PIPEDA, please see "A Guide for Business and Organizations" online at http://www.priv.gc.ca/information/guide_e.cfm

[2] By "third party", we mean the person who is not the subject of surveillance.

May 2009