updated January, 2014

Public Sector Surveillance Guidelines

Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

Public Sector Video Surveillance Guidelines

Purpose

The purpose of this guidance document is to provide information on how the *Freedom of Information and Protection of Privacy Act* ("FIPPA") applies to the use of video and audio surveillance systems by public bodies. In the decade since our office first published surveillance guidelines, there has been extensive research and writing on this topic and one thing is clear: the effectiveness of a surveillance system is a product of several elements—it is not a "one size fits all" solution. These guidelines aim to assist public bodies in deciding whether proposed or existing surveillance systems are ***lawful*** and operating in a ***privacy protective manner.*** These guidelines also set out what the Information and Privacy Commissioner for British Columbia expects from public bodies who are considering using video and audio surveillance systems.

The Right of Privacy

British Columbians are increasingly subject to routine and random surveillance of their ordinary, lawful public activities by public and private bodies. As surveillance increases, so do the risks of harm to individuals. Video and audio surveillance systems are particularly privacy intrusive measures because they often subject individuals to continuous monitoring of their everyday activities.

Privacy is a fundamental right. Sections 7 and 8 of the *Canadian Charter of Rights and Freedoms* protect the rights of citizens to be secure in their daily lives and to be free from unjustified intrusion. FIPPA also recognizes and protects an individual's privacy

rights. Public bodies must not take steps to erode the right to privacy merely because they believe there is nothing to fear if an individual has nothing to hide. The loss of the ability to control the use of one's own personal information is harmful in itself.

APPLICATION OF FIPPA AND ROLE OF THE OIPC

FIPPA governs the collection, use, and disclosure of personal information by public bodies. Visual or audio recordings of an individual are a record of that individual's personal information. Where a surveillance system records personal information, the public body collecting that record must comply with the privacy protection provisions in Part 3 of FIPPA.

The Office of the Information and Privacy Commissioner ("OIPC") is responsible for monitoring and enforcing compliance with FIPPA, and may conduct investigations and audits of public bodies' surveillance systems under the authority of s. 42(1)(a) of FIPPA.

LAWFUL COLLECTION AND USE

It is lawful for public bodies to collect personal information only in circumstances permitted by s. 26 of FIPPA. A public body must be prepared to demonstrate to the OIPC, with specific evidence, that one or more provisions of s. 26 of FIPPA authorize its proposed or existing collection of personal information by a surveillance system.

Each component of the surveillance system must be lawful. For example, if a public body is considering implementing a surveillance system that collects video and audio footage, it should be able to demonstrate the purpose and the legal authority for both. This should include evidence that supports how each component fulfils the purpose for the collection.

Section 32 of FIPPA limits the purpose for which a public body can use personal information. Public bodies should be prepared to demonstrate that the ways they are using personal information meet the requirements of s. 32. Information collected through video or audio surveillance should not be used beyond the original purpose for the collection and any other purpose that is demonstrably consistent with this purpose. When public bodies collect personal information for one reason and then later use it for something else, privacy advocates refer to this as "function creep". Function creep is problematic because it can lead to public bodies using personal information in ways that do not meet the requirements of FIPPA. For example, if a public body scans employee identification to control entry to a secure building and later wants to use it to track employee attendance; the public body must first determine whether FIPPA authorizes that new activity.

- ***WHAT IS PERSONAL INFORMATION?***

FIPPA defines "personal information" as recorded information about an identifiable individual, other than contact information. Video and audio recordings of an individual's image and voice are considered identifiable information.

- ***WHAT IS COLLECTION?***

In terms of surveillance systems, collection of personal information occurs when an individual's image or voice is captured by the system. The personal information may then be played back or displayed on a monitor (used), saved or stored (retained) or shared with other public bodies or organizations (disclosed). Surveillance systems are collecting personal information whenever they are recording, regardless of if, or how, the public body uses, retains or discloses the recordings in the future.

- ***WHAT DOES IT MEAN TO BE AUTHORIZED BY STATUTE?***

Section 26(a) of FIPPA allows for the collection of personal information that is expressly authorized by statute. This is the most straightforward legal authority for collection. If there is a law that states that a public body is authorized to collect personal information using video or audio recording, then, so long as the collection is done in accordance with that law and for the specified purpose, it is authorized.

An example of express statutory authority for video surveillance is found in s. 85 of the Gaming Control Act. Under this section, the British Columbia Lottery Corporation "may place a gaming site under video surveillance to ascertain compliance" with the Act.

- ***WHAT DOES IT MEAN TO BE "FOR THE PURPOSES OF LAW ENFORCEMENT"?***

Section 26(b) of FIPPA authorizes collection of personal information for the purposes of law enforcement. Schedule 1 of FIPPA defines "law enforcement" as: policing, including criminal intelligence systems; investigations that lead or could lead to a penalty or sanction being imposed; or proceedings that lead, or could lead, to a penalty or sanction being imposed.

"Policing" is not defined in FIPPA, however in common law the definition of policing involves active monitoring or patrolling in order to deter or intervene in unlawful activities. Information collected for policing purposes must be collected by a public body with a common law or statutory enforcement mandate. For example, it is not sufficient for a public body to claim an interest in reducing crime in order to justify

collection for "law enforcement"; the public body must have authority to enforce those laws.

In BC, the OIPC has determined in a number of Orders that an investigation must already be underway at the time the personal information is collected for s. 26(b) to apply. A public body is not authorized to collect personal information about citizens, in the absence of an investigation, on the chance it may be useful in a future investigation. Similarly, in order for a collection to be lawfully authorized as relating to a proceeding, the proceeding must be ongoing at the time of collection.

- ***WHAT DOES IT MEAN TO BE "NECESSARY"?***

Section 26(c) of FIPPA authorizes the collection of personal information that is necessary for an operating program or activity of the public body. "Necessary" in the context of surveillance systems is a high threshold for a public body to meet. It is not enough to say that personal information would be nice to have or could be useful in the future. The personal information must also be directly related to a program or activity of the public body.

- ***WHAT ABOUT CONSENT?***

Under s. 26(d)(i) of FIPPA, consent can be used as legal authority for collection of personal information in very few specified instances. Express or implied consent is not a legal authority for collection of personal information using video or audio surveillance systems.

EFFECTIVE USE OF SURVEILLANCE

A public body should use a video or audio surveillance system only where conventional means for achieving the same objectives are *substantially* less effective than surveillance *and* the benefits of surveillance *substantially* outweigh any privacy intrusion. Cost-savings alone are not sufficient justification to proceed with a surveillance system under FIPPA.

A public body should use surveillance systems that collect the minimum amount of personal information necessary to achieve the purpose of the collection.

In considering the effectiveness of video or audio surveillance systems, public bodies should keep in mind the following:

(a) Surveillance systems have been found to be more effective in defined areas (such as parking lots) as opposed to open street or undefined spaces.

(b) Surveillance systems are *more effective as investigative tools than as deterrents*. There is a common belief that the presence of a camera is an effective deterrent of crime and disorder, however, studies have shown that this deterrence is short-lived. In addition, the deployment of a surveillance system often coincides with the installation of improved lighting and increased monitoring of the area, which itself plays a role in deterrence.

(c) Surveillance systems that are monitored and are used in conjunction with intervention in suspicious incidents have been found to be more effective at reducing criminal or public safety concerns than are unmonitored systems.

Public bodies should only proceed with surveillance if they can first establish whether FIPPA authorizes the surveillance and if they have determined that other less privacy-invasive options will not be effective.

VIDEO OR AUDIO SURVEILLANCE –– BEST PRACTICES

1. Factors in considering use of video or audio surveillance systems

Public bodies should take the following steps in considering whether to use video or audio surveillance systems:

(a) Before implementing a surveillance system, complete a privacy impact assessment ("PIA"). A PIA is an important component in the design of a project to assess how the project affects the privacy of individuals, and should include a description of measures to mitigate any identified privacy risks. Completion of a PIA helps a public body ensure that its project complies with the legislative requirements under FIPPA. A copy of the completed PIA, including the public body's case for implementing a surveillance system as opposed to other measures, should be sent to the OIPC for review and comment. The OIPC should receive the PIA *well before* any final decision is made to proceed with surveillance.

(b) If a public body would like to use surveillance for security reasons, it should have evidence, such as verifiable, specific reports of incidents of crime, public safety concerns or other compelling circumstances that support the necessity of surveillance.

(c) Conduct consultations with stakeholders who may be able to help the public body consider the merits of the proposed surveillance.

(d) Calibrate the surveillance system so that it only collects personal information that is necessary to achieve the purposes the public body has identified for the surveillance.

2. Layout of surveillance equipment

In designing a surveillance system and installing equipment, a public body should:

(a) Install surveillance equipment such as video cameras or audio recording devices in defined public areas. The public body should select areas it expects the surveillance will be most effective in meeting the purpose for the surveillance.

(b) Recording equipment should not be positioned, internally or externally, to monitor areas outside a building, or to monitor other buildings, unless necessary to accomplish the purpose for the surveillance. Cameras should not be directed to look through the windows of adjacent buildings. Equipment should not monitor areas where the public and employees have a reasonable expectation of privacy (such as change rooms and washrooms).

(c) If the purpose of the surveillance is related to crime, the public body should restrict the use of surveillance to periods when there is demonstrably a higher likelihood of crime being committed and detected in the area under surveillance.

(d) Section 27(2) of FIPPA requires that public bodies notify individuals when they are collecting personal information. A public body should notify the public, using clearly written signs prominently displayed at the perimeter of surveillance areas so the public has sufficient warning that video or audio surveillance is or may be in operation before entering any area under surveillance. The notification must state: the purpose for the collection, the legal authority for the collection, and the title, business address and business telephone number of an employee of the public body who can answer the individual's questions about the collection.

(e) Only authorized persons should have access to the system's controls and to its reception equipment (such as video monitors or audio playback speakers). Public bodies should have policies in place to ensure that authorized persons only access personal information from a surveillance system for authorized purposes.

(f) Recording equipment should be in a controlled access area. Video monitors should not be located in a position that enables public viewing. Only authorized employees should have access.

3. Guidelines regarding surveillance records

Section 30 of FIPPA requires that a public body protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized collection, access, use, disclosure or disposal. If the surveillance system creates a record, a public body should implement the following security policies and procedures:

3.1 Access

(a) Only authorized individuals who require the information in order to do their jobs should have access to the surveillance system or the records it creates. All authorized personnel should be fully aware of the purposes of the system and fully trained in rules protecting privacy.

(b) Access to storage devices should be possible only by authorized personnel. Logs should be kept of all instances of access to, and use of, recorded material.

(c) An individual who is the subject of surveillance has a right to request access to his or her recorded personal information under s. 5 of FIPPA. Normally, FIPPA requires public bodies to withhold personal information about other individuals. This may mean that a public body must blur or otherwise obfuscate the identity of other individuals on a video or audio recording before disclosing personal information about an individual. Public body policies and procedures should be designed to accommodate this right to seek access.

3.2 Disclosure for law enforcement purposes

(a) If a public body is disclosing records containing personal information for law enforcement purposes, it should complete an information release form first. The form should indicate who took the storage device containing the information, under what authority, when this occurred, and if it will be returned or destroyed after use.

3.3 Secure retention and disposal

(a) A public body must securely store, or retain, all personal information in its custody or under its control, including audio and video recordings. This includes the following measures:

i. All electronic storage devices should be encrypted.

ii. All electronic storage devices that are not in use should be stored securely in a locked receptacle located in a controlled access area. All storage devices that have been used should be numbered and dated.

iii. Recorded information should be erased according to a standard retention and disposal schedule. The OIPC considers retention periods of not more than 30 days to be preferable, although circumstances may necessitate different retention periods.

iv. If the recorded information reveals an incident that contains personal information about an individual, and the public body uses this information to make a decision that directly affects the individual, s. 31 of FIPPA requires that specific recorded information be retained for one year after the decision is made.

(b) A public body must securely dispose of old storage devices and records.

4. Audit procedures

As part of the requirement to secure personal information, public bodies should ensure employers and contractors are aware of, and implement, the following audit procedures:

(a) All surveillance equipment operators must be aware that their operations are subject to audit and that they may be called upon to justify their surveillance interest in any given individual.

(b) A public body should appoint a review officer to audit the use and security of surveillance equipment, including monitors and storage devices. The reviews should be done periodically at irregular intervals. The results of each review should be documented in detail and any concerns should be addressed promptly and effectively.

5. Creating surveillance system policies

(a) If a public body makes a decision to use a video or audio surveillance system, it should do so in accordance with a comprehensive policy that ensures compliance with FIPPA. Such a policy is one part of an overall privacy management program. Some of the key privacy issues that public bodies should address through policies include:

i. Authority for collection, use and disclosure of personal information;

ii. Requirements for notification.

iii. Individual access to personal information.

iv. Retention and disposal of information.

v. Responsible use of information and information technology, including administrative, physical and technological security controls and appropriate access controls.

vi. A process for handling privacy related complaints.

(b) The public body should designate one (preferably senior) person to be in charge of the system as well as the public body's privacy obligations under FIPPA and its policies. Any power for that person to delegate his or her role should be limited, and should include only other senior staff.

(c) Employees and contractors should be required to review and apply the policies in performing their duties and functions related to operation of the surveillance system. Employees should be subject to discipline if they breach the policies or the relevant FIPPA provisions. Where contractors are used, failure to comply with the policies, or FIPPA's provisions should be a breach of contract leading to penalties up to and including contract termination. Employees and contractors (and contractor employees) should sign written agreements as to their duties under the policies.

(d) Public bodies should incorporate policies into personnel training and orientation programs and should require contractors to do the same with their employees. Policies should be regularly reviewed and updated as needed, ideally at least once every two years. Public body and contractor personnel should receive privacy awareness training at least annually. Public bodies should be able to demonstrate how and when they trained their staff.

For more information on public sector privacy management, see the OIPC's guidance document: *Accountable Privacy Management in BC's Public Sector.*[1]

6. On-going evaluation

The effectiveness of a video or audio surveillance system should be regularly evaluated by independent evaluators. Some considerations for evaluation include:

(a) Taking special note of the initial reasons for undertaking surveillance and determine whether video surveillance has in fact addressed the problems identified.

(b) Reviewing whether a video or audio surveillance system should be terminated, either because the problem that justified its use in the first place is

[1] http://www.oipc.bc.ca/guidance-documents/1545

no longer significant, or because the surveillance has proven ineffective in addressing the problem.

(c) Taking account of the views of different groups in the community (or different communities) affected by the surveillance. Results of evaluations should be made publicly available.

CONCLUSION

Video and audio surveillance systems are inherently privacy invasive. In order for a public body to use surveillance, it must first establish that FIPPA authorizes the use. Even if surveillance is authorized, a public body should determine whether there are other, less privacy invasive options. This document is intended to assist public bodies in assessing whether video or audio surveillance is an appropriate solution to their identified problem and, if it is, to help them design and implement surveillance in accordance with FIPPA and best practices.

If you have any questions about these guidelines, please contact:

Office of the Information and Privacy Commissioner for BC
Tel: (250) 387-5629
In Vancouver: (604) 660-2421; Elsewhere in BC: 1-800-663-7867
Email: info@oipc.bc.ca

For more information regarding the OIPC, please visit www.oipc.bc.ca.

NOTE: These guidelines do not constitute a decision or finding by the OIPC respecting any matter within the jurisdiction of the Information and Privacy Commissioner under the Act. These guidelines do not affect the powers, duties or functions of the Information and Privacy Commissioner respecting any complaint, investigation or other matter under or connected with the Act and the matters addressed in this document.

Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

Office of the Information and Privacy Commissioner for British Columbia

PO Box 9038, Stn. Prov. Govt. Victoria, BC V8W 9A4 | Telephone: 250.387.5629 | Toll free in B.C. 1.800.663.7867
E-mail: info@oipc.bc.ca | www.oipc.bc.ca | Twitter: @BCInfoPrivacy