



## **PUBLIC SURVEILLANCE SYSTEM PRIVACY GUIDELINES**

**OIPC REFERENCE DOCUMENT 00-01**

**January 26, 2001  
(Replaces: June 21, 2000)**

*Text changes from the immediately preceding version of this document are italicized.*

### **1.0 PURPOSE OF THIS DOCUMENT**

There is a very real risk that within a few short years British Columbians could find themselves subjected to pervasive, routine and random surveillance of their ordinary, lawful public activities. Surveillance systems have, in recent years, proliferated; they are operated by a wide variety of public and private bodies. The result is widespread surveillance of our ordinary lives. There is a very real prospect that this will evolve into a blanket system of automated surveillance. In and of itself, each system might be lawful and reasonable, but the synergy of all systems operating together is something the public is likely to regret.

It is not sufficient to say that citizens need not fear surveillance if they have nothing to hide. This misses the point. Privacy is a fundamental human and civil right that has constitutional dimensions, under ss. 7 and 8 of the *Canadian Charter of Rights and Freedoms*. It is also recognized, and protected, by the *Freedom of Information and Protection of Privacy Act* ("Act"). The right to privacy must not be eroded simply because there is supposedly nothing to fear if you have nothing to hide. Citizens have the right to feel, and to be, secure in their daily lives, but they also have the right to be free of unwarranted intrusion into their lives.

These guidelines are designed to assist public bodies in deciding whether collection of personal information by means of a video, audio or other mechanical or electronic surveillance system is both lawful *and* justifiable as a policy choice and, if so, how privacy protection measures should be built into the system. The Office of the Information and Privacy Commissioner ("OIPC") strongly encourages all public bodies that use, or are considering the use of, surveillance systems to comply with these guidelines.

These guidelines are intended to apply to surveillance systems in open public spaces (including streets, highways, parks) and public buildings (including government buildings, libraries, hospitals and educational institutions). They do not deal with workplace surveillance issues arising where a public body employer wishes to engage in surveillance of employees. Workplace surveillance issues will be addressed in a future OIPC publication.

These guidelines also apply, in a more limited manner, to covert surveillance. Covert surveillance is surveillance that is conducted through the use of hidden recording devices. It can be a highly intrusive and privacy invasive form of surveillance due to its secretive nature. A detailed and comprehensive assessment must be conducted prior to the decision to implement covert surveillance, to ensure that it is the only available option and that benefits derived from the material obtained far outweigh the violation to the privacy rights of the subjects being observed. If a public body regularly engages in covert surveillance as a case-based investigative tool for law enforcement purposes (including detection of insurance or other fraud) it should have a protocol in place that establishes the decision-making process to be followed before it is used in a given case. The guidelines in this paper, except those related to notification, placement of equipment and the preparation of a Privacy Impact Assessment, will still apply to covert surveillance. If a public body is undertaking a new form of covert surveillance, consultation with the OIPC should take place and a Privacy Impact Assessment should be developed respecting the new form of covert surveillance.

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.

## **2.0 OUR ROLE**

All public bodies covered by the Act are required to comply with the privacy protection provisions of Part 3 of the Act. Those provisions govern the collection, use, storage and disclosure of personal information by public bodies. The Act defines personal information as recorded information about an identifiable individual. Personal information includes race, ethnic origin, colour, age, and sex. Any record of the image of an identifiable individual, including the characteristics of race, ethnic origin, colour, age, or sex, is a record of personal information.

Where a surveillance system records visual or audio information that is personal information, the record, and the public body's practices respecting that personal information, are subject to the privacy protection provisions in Part 3 of the Act. The OIPC has a regulatory role in monitoring and enforcing compliance with those provisions. The OIPC may conduct audits of public bodies' surveillance systems under the authority of s. 42(1)(a) of the Act. These audits will review public bodies' compliance with the Act's requirements.

### **3.0 GENERAL COMMENTS AND CONCERNS**

It is lawful for public bodies to collect personal information only in circumstances permitted by s. 26 of the Act. Before a public body can lawfully implement a surveillance system, any resulting collection of personal information must be expressly authorized by statute (s. 26(a)), must be for the purposes of "law enforcement" as defined in the Act (s. 26(b)), or must relate directly to and be necessary for an operating program or activity of the public body (s. 26(c)). The Act 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. A public body must be prepared to demonstrate to the OIPC, with specific evidence, that its proposed or existing collection of personal information by surveillance system is authorized under the Act in one of the ways just described.

More important from a public policy perspective, the OIPC considers the effectiveness of public surveillance systems for law enforcement purposes to be open to question in almost all cases. As is noted below in section 4.1(a), a surveillance system should be used only where conventional means for achieving the same law enforcement objectives are *substantially* less effective than surveillance *and* the benefits of surveillance *substantially* outweigh any diminution of privacy inherent in the system's existence and use. Cost-savings alone are not, in the OIPC's view, sufficient justification to proceed with a surveillance system. Surveillance systems are not a cure-all. Their privacy implications require extreme caution and avoidance of their use is desirable wherever possible, even where they are lawful. Further, where surveillance is used, the system should be designed so that it creates the least possible privacy impacts.

### **4.0 GUIDELINES**

#### **4.1 Factors In Considering Use of Surveillance**

In considering whether to use surveillance, public bodies should take the following steps:

- 
- (a) A public body should only use surveillance as a last resort. Other measures of deterrence or detection must be considered before surveillance is entertained as a solution. A surveillance system should be used only where conventional means for achieving the same law enforcement objectives are *substantially* less effective than surveillance *and* the benefits of surveillance *substantially* outweigh any diminution of privacy inherent in the system's existence and use. A public body should be prepared to demonstrate that these factors have been satisfied.
  - (b) Public bodies must be prepared to justify the use of a surveillance system on the basis of verifiable, specific reports of incidents of crime, public safety concerns or other compelling circumstances.
  - (c) Before implementing a surveillance system, a public body should complete a Privacy Impact Assessment ("PIA"), to assess the actual or potential effects the proposed surveillance may have on privacy and on the ways in which any adverse effects are to be mitigated. The OIPC has developed a model privacy impact assessment and a blank assessment form for use by public bodies. These documents are available at [http://www.oipc.bc.ca/sector\\_public/resources/pia.htm](http://www.oipc.bc.ca/sector_public/resources/pia.htm)
  - (d) A copy of the completed PIA, together with the public body's case for implementing a surveillance system as opposed to other measures, as outlined in this section, should be sent to the OIPC, to the attention of the Executive Director, for review and comment. These documents should be received by the OIPC *well before* any final decision is made to proceed with surveillance.
  - (e) It is recommended that the public body consider conducting consultations with relevant stakeholders, who may be able to assist the public body in making an informed decision as to the necessity for, and acceptability to the public, of the proposed surveillance.
  - (f) The implemented surveillance system should be designed and operated so that the privacy intrusion it creates is no greater than is absolutely necessary to achieve the system's goals.

## 4.2 Creating Surveillance System Policies

Once a decision is made to use a surveillance system, the public body should do the following in creating and implementing a policy for operation of the system:

- (a) The public body should develop a comprehensive written policy to govern the use of the system's equipment. The policy should address the location of recording equipment, which personnel are authorized to operate the

system, the times when surveillance will be in effect, and the location of reception equipment (*i.e.*, the place where audio, visual or other signals received through the system are monitored). Where the system creates a record, the policy should also deal with the matters discussed in section 4.4, below.

- (b) The policy should designate one (preferably senior) person to be in charge of the system, including as regards the public body's privacy obligations under the Act and the policy. Any power for that person to delegate his or her role should be limited, and should include only other senior staff.
- (c) The public body should require employees and contractors to review and apply the policy in performing their duties and functions related to operation of the surveillance system. Employees should be subject to discipline if they breach the policy or the relevant Act provisions. Where contractors are used, failure to comply with the policy, or the Act'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 policy.
- (d) The policy should be incorporated into personnel training and orientation programs and contractors should be required to do the same with their employees. Public body and contractor personnel should periodically (preferably annually) have their awareness of the policy and Act refreshed. The policy itself should be reviewed regularly and updated as needed, ideally at least once every two years.

### **4.3 Layout of Surveillance Equipment**

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

- (a) Installation of recording equipment such as video cameras or audio recording devices should be restricted to identified public areas. Areas chosen for surveillance should be those where surveillance is a necessary and viable deterrent, as contemplated by section 4.1(a). Recording equipment should not be positioned, internally or externally, to monitor areas outside a building, or to monitor other buildings, unless necessary to protect external assets or ensure personal safety. 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 adult or *children's* washrooms). (This requirement may not always apply where covert surveillance is used. See Part 1.0, above.)

- (b) A public body should restrict use of surveillance to periods when there is demonstrably a higher likelihood of crime being committed and detected in the area under surveillance.
- (c) A public body should notify the public, using clearly written signs prominently displayed at the perimeter of surveillance areas, of surveillance equipment locations, so the public has ample warning that surveillance is or may be in operation before entering any area under surveillance. (Public bodies should remember that signs almost certainly serve as a general deterrent.) This requirement does not apply to covert surveillance. A public body's signs should identify someone who can answer questions about the surveillance system. An address or telephone number should be given for the contact person.
- (d) Only authorized persons should have access to the system's controls and to its reception equipment.
- (e) Receiving equipment (such as video monitors or audio playback speakers) should be in a controlled access area. Only the controlling personnel, or those properly authorized in writing by those personnel according to the public body's policy, should have access to the receiving equipment. Video monitors should not be located in a position that enables public viewing.

#### **4.4 Guidelines Regarding Surveillance Records**

If the surveillance system creates a record, the following policies and procedures for access, use, disclosure, retention and destruction should be implemented (and should form part of the policy discussed in section 4.2):

- (a) All tapes or other storage devices (such as computer disks or chips) 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.
- (b) Access to the 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) A public body should develop written policies on the use and retention of recorded information that address all of the following:
  - (i) Under what circumstances information is viewed and by whom. (For example, are all recordings viewed routinely or only when an incident is reported? Who is authorized to view the recordings?) The public body's personnel should only view information where there is

a need to do so, either because an incident has been reported or is suspected to have occurred.

- (ii) If viewing the information reveals no incident, or no incident is reported, how long is the recorded information retained? Recorded information should be routinely erased where no incident has been reported, or where viewing the recorded information reveals no incident, according to a standard schedule (e.g., every 24 hours, 48 hours or week). The OIPC considers retention periods of not more than 30 days to be preferable, although circumstances may necessitate different retention periods.
  - (iii) When the recorded information reveals an incident, how long is it retained? (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 the Act requires the recorded information to be retained for one year after the decision is made.)
- (d) A public body should retain and store storage devices required for evidentiary purposes according to standard procedures until law enforcement authorities request them. A storage device release form should be completed before any storage device is disclosed to appropriate authorities. The form should indicate who took the device, under what authority, when this occurred, and if it will be returned or destroyed after use.
- (e) 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 the Act. Access in full or in part may be refused on one of the grounds set out in Division 2 of Part 2 of the Act. However, if that information can reasonably be severed from a record, an applicant has the right of access to the remainder of the record. Public body policies and procedures should be designed to accommodate this right to seek access.
- (f) A public body must securely dispose of old storage devices. Physically breaking open a videotape cassette, audiotape, or computer disk is not sufficient. The storage media should be shredded, burned or magnetically erased.

#### **4.5 Audit Procedures**

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.

