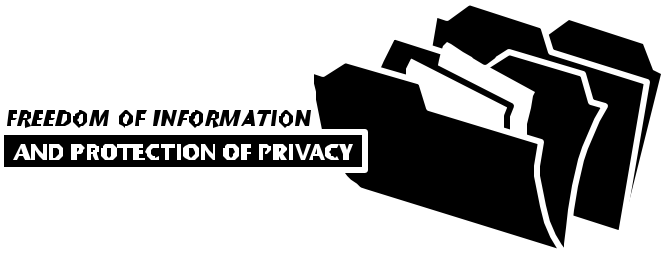

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY

Guide to Using Surveillance Cameras in Public Areas

April 2001

ISBN 0-7785-1441-2

Alberta
GOVERNMENT OF ALBERTA

Information Management and Privacy Branch
Alberta Government Services
16th Floor, Commerce Place
10155 – 102 Street
Edmonton, Alberta
Canada, T5J 4L4
Phone: (780) 422-2657
Fax: (780) 427-1120
E-mail: foiphelpdesk@gov.ab.ca

FOIP Help Desk: (780) 427-5848
Toll free dial 310-0000
E-mail: foiphelpdesk@gov.ab.ca

For more information on Alberta's Freedom of Information and Protection of Privacy (FOIP) legislation:

Information Management and Privacy Branch Web Site: http://www.gov.ab.ca/foip
Publications, including

- *The Right to Information and the Right to Privacy* pamphlet
- *FOIP: A Guide*
- *FOIP Guidelines and Practices*
- *FOIP Implementation Checklist*
- *Contractor's Guide to the FOIP Act*
- *Contract Manager's Guide*
- *Guide for Developing Personal Information Sharing Agreements*
- Legislation
- FOIP Coordinators/Contacts
- Information and Privacy Commissioner's Orders and Investigation Reports
- Frequently Asked Questions

Queen's Printer
Edmonton: (780) 427-4952
Calgary: (403) 297-6251
Website: http://www.gov.ab.ca/qp

- *FOIP Act and Regulation*
- *FOIP Guidelines and Practices*
- *Annotated FOIP Act*
- *The Right to Know, The Right to Privacy* videotape

Office of the Information and Privacy Commissioner
410, 9925 - 109 Street
Edmonton, Alberta T5K 2J8
Phone: (780) 422-6860
Fax: (780) 422-5682
E-mail: ipcab@planet.eon.net
Web Site: http://www.oipc.ab.ca

Freedom of Information and Protection of Privacy

Guide to Using Surveillance Cameras in Public Areas

Table of Contents

ACKNOWLEDGMENTS

This *Guide* is based upon and imports many of the policies and guidelines outlined in the British Columbia Office of the Information and Privacy Commissioner's *Public Surveillance System Privacy Guidelines*, OIPC Policy 00-01, June 21, 2000. That contribution is gratefully acknowledged.

Input and advice on the content of the *Guide* was also received from the Office of the Information and Privacy Commissioner of Alberta. The contribution of that Office is also gratefully acknowledged.

1. INTRODUCTION

Surveillance cameras can be an effective technique to protect public safety and detect or deter criminal activity. Surveillance cameras are increasingly being installed inside and outside of public buildings (in elevators, hallways, entrances, etc.), on streets, highways, in parks and public transportation vehicles.

Public bodies subject to the *Freedom of Information and Protection of Privacy (FOIP) Act* must balance the benefits to the public against the rights of individuals to be left alone. A key issue in privacy protection is the regulation of the collection of personal information, thereby preventing unnecessary surveillance of individuals.

This guide is intended to assist public bodies in deciding whether collection of personal information by means of a surveillance camera is both lawful and justifiable and, if so, in understanding how privacy protection measures can be built into the use of a surveillance system.

The guidelines do not apply to covert or overt surveillance cameras being used by a public body as a case-specific investigation tool for law enforcement purposes, where there is statutory authority and/or the authority of a search warrant to conduct the surveillance.

They are also not intended to apply to workplace surveillance systems installed by a public body employer to conduct surveillance of employees.

Other considerations may apply to this type of surveillance and will not be covered in this guide.

2. DEFINITIONS

In this guide:

"Covert Surveillance" refers to "the secretive continuous or periodic observation of persons, vehicles, places or objects to obtain information concerning the activities of individuals, which is then recorded in material form, including notes and photographs". [1]

"Personal Information" is defined in **section 1(1)(n)** of the *FOIP Act* as recorded information about an identifiable individual, including: the individual's race, colour, national or ethnic origin; the individual's age or sex; the individual's inheritable characteristics; information about an individual's physical or mental disability; and any other identifiable characteristics listed in that section.

"Surveillance System" refers to a mechanical or electronic system or device that enables continuous or periodic video recording, observing or monitoring of personal information about individuals in open, public spaces (including streets, highways, parks), public buildings (including provincial and local government buildings, libraries, health care facilities, public housing and educational institutions) or public transportation, including school

[1] *Covert Surveillance in Commonwealth Administration: Guidelines, Human Rights and Equal Opportunity Commission, February, 1992*

and municipal transit buses or other similar vehicles.

"Reception Equipment" refers to the equipment or device used to receive or record the personal information collected through a public surveillance system, including a camera or video monitor.

"Record" is defined in **section 1(1)(q)** of the *FOIP Act* as a record of information in any form and includes books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records. In the context of this *Guide*, "record" includes digitally recorded or stored media such as images on videotape.

"Storage Device" refers to a videotape, computer disk or drive, CD ROM or computer chip used to store the recorded visual images captured by a surveillance system.

3. COLLECTING PERSONAL INFORMATION USING SURVEILLANCE CAMERAS

Any record of the image of an identifiable individual is a record of personal information. Since surveillance systems collect personal information about identifiable individuals, public bodies must determine if they have the authority to collect personal information under **section 32** of the *FOIP Act*.

Under that section, no personal information may be collected by or for a public body unless the collection is expressly authorized by an enactment of Alberta or Canada **(section 32(a))**; the information is collected for the purposes of law enforcement **(section 32(b))**; or the information relates directly to and is necessary for an operating program or activity of the public body **(section 32(c))**.

Public bodies must be able to demonstrate to the Information and Privacy Commissioner that any proposed or existing collection of personal information by surveillance cameras is authorized under one of the above sections of the *Act*.

4. CONSIDERATIONS PRIOR TO USING SURVEILLANCE CAMERAS

In order to comply with **Part 2** of the *FOIP Act*, the *FOIP Guidelines and Practices* publication recommends that public bodies consider the following before deciding to use surveillance:

- Surveillance cameras should be used only where conventional means for achieving the same objectives are substantially less effective than surveillance and the benefits of surveillance substantially outweigh any reduction of privacy in the existence and use of the system.

- The use of a surveillance camera should be able to be justified on the basis of verifiable, specific reports of

incidents of crime (e.g., vandalism, theft), safety concerns or other compelling circumstances.

- A Privacy Impact Assessment (PIA) should be completed to assess the effects that the proposed surveillance system may have on privacy and the ways in which any adverse effects can be mitigated (see Chapter 9).

- Consultations may be conducted with relevant stakeholders as to the necessity, and acceptability to the public, of the proposed surveillance.

- Ensure that the proposed design and operation of the system creates no greater privacy intrusion than is absolutely necessary to achieve its goals.

- Prior to deciding to use covert surveillance for a purpose other than a case-specific law enforcement activity, public bodies should conduct a comprehensive PIA and provide it, together with the case for implementing covert surveillance to the Office of the Information and Privacy Commissioner.

  The purpose of the PIA is to ensure that covert surveillance is the only available option and that the benefits derived from the personal information obtained would far outweigh the violation of privacy of the individuals observed.

  A public body that regularly uses covert surveillance as a case-specific investigation tool for law enforcement purposes may, as part of sound privacy protection practices, consider developing a protocol that establishes how the decision is made to use covert surveillance in a given case. The protocol could also include privacy protection practices for the operation of the system.

5. DEVELOPING A SURVEILLANCE SYSTEM POLICY

Once a decision has been made to use a surveillance system, a public body should consider developing and implementing a policy for the operation of the system. Such a policy should be written and should include:

- the use of the system's equipment, including 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. Where the system creates a record, the policy should also deal with the access, use, disclosure, retention and destruction of those records (see Chapter 7);

- the designation of a senior person to be responsible for the public body's privacy obligations under the *Act* and the policy. Any delegation of the individual's responsibilities should be limited and should include only other senior staff;

- a requirement that employees and contractors review and comply with 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 provisions of the *FOIP Act* or other relevant statute. Where a contractor fails to comply with the policy or the provisions of the *Act*, it would be considered a breach of contract leading to penalties up to and including contract termination. Employees and contractors (and their employees) should sign written agreements regarding their duties under the policy;

- the incorporation of the policy into personnel (and contractor's employee) training and orientation programs. Public body and contractor personnel should periodically have their awareness of the policy and *Act* refreshed. The policy should be reviewed and updated regularly, ideally once every two years.

6. DESIGNING AND INSTALLING SURVEILLANCE EQUIPMENT

In designing a surveillance system and installing equipment, the following guidelines should be kept in mind:

- Recording equipment such as video cameras should be installed in identified public areas where surveillance is a necessary and viable detection or deterrence activity.

- 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 to 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 (e.g., change rooms and adult washrooms). Note that there may be situations where surveillance equipment may need to be installed close to or at an entry to a children's washroom in a public building to monitor or deter potential criminal activity against children.

- The use of surveillance should be restricted to periods when there is a demonstrably higher likelihood of crime being committed and detected in the area under surveillance.

- The public should be notified, 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.

  The signs should identify someone who can answer questions about the surveillance system and include an address or telephone number for contact purposes.

- Only authorized persons should have access to the system's controls and to its reception equipment.

- Reception equipment should be in a controlled access area. Only the controlling personnel, or those properly authorized in writing by those personnel according to the policy of the public body, should have access to the reception equipment. Video monitors should not be located in a position that enables public viewing.

7. ACCESS, USE, DISCLOSURE, RETENTION AND DESTRUCTION OF SURVEILLANCE RECORDS

If the surveillance system creates a record by recording visual information that is personal information, the following policies and procedures should be implemented by public bodies and should form part of the policy discussed in Chapter 5:

- All tapes or other 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.

- Access to the storage devices should only be by authorized personnel. Logs should be kept of all instances of access to, and use of, recorded material.

- Written policies on the use and retention of recorded information should cover:

  - who can view the information and under what circumstances? (e.g., because an incident has been reported or is suspected to have occurred);

  - how long the information should be retained where viewing reveals no incident or no incident has been reported? (e.g., information should be erased according to a standard schedule). The Office of the Information and Privacy Commissioner in British Columbia suggests that retention periods of not more than 30 days are preferable.[2]

  - how long the information should be retained if it reveals an incident? (e.g., if the personal information is used to make a decision that directly affects the individual, **section 34** of the *Act* requires the recorded information to be kept for at least one year after the decision is made).

- If the surveillance system has been installed for public safety or deterrence purposes but detects possible criminal activity or non-compliance with or breach of a statute that could lead to a penalty or sanction under an enactment of Alberta or Canada, the storage devices required for evidentiary purposes should be retained and stored according to standard

[2] *Public Surveillance System Privacy Guidelines, Office of the Information and Privacy Commissioner, British Columbia, OIPC Policy 00-01, June 21, 2000*

procedures until law enforcement authorities request them.

A storage device release form should be completed before any storage device is disclosed to such authorities. The form should state who took the device and when, under what authority, and if it will be returned or destroyed after use.

- An individual who is the subject of the information has a right of access to his or her recorded information under **section 6** of the *Act*. Policies and procedures should accommodate this right. Access may be granted in full or in part depending upon whether any of the exceptions in **Division 2, Part 1** of the *Act* apply and whether the excepted information can reasonably be severed from the record.

- Old storage devices must be securely disposed of by shredding, burning or magnetically erasing the information. Breaking open the storage device is not sufficient

8. AUDITING THE USE OF SURVEILLANCE SYSTEMS

Public bodies should:

- ensure that their employees and contractors are aware that their operations are subject to audit and that they may have to justify their surveillance interest in any individual. An audit clause should be added to any contract for the provision of surveillance services;

- ensure that they appoint a review officer to periodically audit, at irregular intervals, the use and security of surveillance equipment, including cameras, monitors and storage devices. The results of each review should be documented and any concerns addressed promptly and effectively.

9. ROLE OF THE INFORMATION AND PRIVACY COMMISSIONER

The personal information recorded by a public body's surveillance system, and the public body's practices respecting the personal information, are subject to the privacy protection provisions in **Part 2** of the *Act*. The Information and Privacy Commissioner can monitor and enforce compliance with those provisions. The Commissioner may also conduct audits of the surveillance systems of public bodies to ensure compliance with the provisions of **Part 2** of the *Act***.**

The Commissioner's methodology and process for Privacy Impact Assessments can be found at www.oipc.ab.ca. Also, see the *FOIP Guidelines and Practices* publication for information on conducting PIAs.

The completed PIA, together with the case for implementing a surveillance system, as opposed to other measures, should be sent to the Office of the

Information and Privacy Commissioner for review and comment early in the process and certainly prior to making a final decision to proceed with surveillance.

Details of the security measures to be implemented for a proposed surveillance system may be placed in an appendix or attachment to the PIA so that they can be kept confidential if the PIA is published by the Commissioner.

If the public body intends to significantly modify or expand the surveillance system, consult with the Office of the Information and Privacy Commissioner. The Commissioner may conduct a site visit to assess the impact of the proposed modification.

BIBLIOGRAPHY

1. *Public Surveillance System Privacy Guidelines,* Office of the Information and Privacy Commissioner, British Columbia, OIPC Policy 00-001, June 21, 2000.

2. *Video Surveillance: The Privacy Implications,* The Information and Privacy Commissioner, Ontario, Practice No. 10.

3. *Video Surveillance by Public Bodies: A discussion,* Investigation Report P98-012, Office of the Information and Privacy Commissioner, British Columbia, March 31, 1998.

4. *Covert Surveillance in Commonwealth Administration: Guidelines,* Human Rights and Equal Opportunity Commission, February 1992.