Information
and Privacy
Commissioner/
Ontario

Guidelines for Using Video Surveillance Cameras in Public Places

Ann Cavoukian, Ph.D.
Commissioner
October 2001

Acknowledgements

These *Guidelines* build on those developed by the British Columbia Information and Privacy Commissioner's *Public Surveillance System Privacy Guidelines,* dated January 26, 2001, and the *Guide to Using Surveillance Cameras in Public Areas,* issued by the Government of Alberta's Freedom of Information and Protection of Privacy Office, dated April 2001. These sources are gratefully acknowledged.

The Information and Privacy Commissioner/Ontario gratefully acknowledges the work of Judith Hoffman in preparing this report.

This publication is also available on the IPC website.

Cette publication est egalement disponible en frangais.

Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Table of Contents

1. Introduction

Government institutions are considering the implementation of video surveillance technology with increasing frequency for the purposes of general law enforcement programs and public safety programs. In limited and defined circumstances, video surveillance cameras may be appropriate to protect public safety and detect or deter criminal activity.

Institutions governed by the *Freedom of Information and Protection of Privacy Act* (the provincial *Act)* and the *Municipal Freedom of Information and Protection of Privacy Act* (the municipal *Act)* that are considering implementing a video surveillance program must balance the benefits of video surveillance to the public against an individual's right to be free of unwarranted intrusion into his or her life. Pervasive, routine and random surveillance of ordinary, lawful public activities interferes with an individual's privacy.

These *Guidelines* are intended to assist institutions in deciding whether the collection of personal information by means of a video surveillance system is lawful and justifiable as a policy choice, and if so, how privacy protective measures can be built into the system.

These *Guidelines* do not apply to surveillance when used 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.

Covert surveillance is surveillance conducted through the use of hidden devices. If covert surveillance is not implemented pursuant to the conditions in the preceding paragraph, extra diligence in considering the use of this technology is required, as set out in Appendix A.

These guidelines are also not intended to apply to workplace surveillance systems installed by an institution to conduct workplace surveillance of employees.

2. Definitions

In these *Guidelines:*

Personal information is defined in section 2 of the *Acts* as recorded information about an identifiable individual, which includes, but is not limited to, information relating to an individual's race, colour, national or ethnic origin, sex and age. If a video surveillance system displays these characteristics of an identifiable individual or the activities in which he or she is engaged, its contents will be considered "personal information" under the *Acts.*

Record, also defined in section 2 of the *Acts,* means any record of information, however recorded, whether in printed form, on film, by electronic means or otherwise, and includes: a photograph, a film, a microfilm, a videotape, a machine-readable record, and any record that is capable of being produced from a machine-readable record.

Video Surveillance System refers to a video, physical or other mechanical, electronic or digital surveillance 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). In these *Guidelines,* the term video surveillance system includes an audio device, thermal imaging technology or any other component associated with capturing the image of an individual.

Reception Equipment refers to the equipment or device used to receive or record the personal information collected through a video surveillance system, including a camera or video monitor or any other video, audio, physical or other mechanical, electronic or digital device.

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

3. Collection of Personal Information Using a Video Surveillance System

Any recorded data or visual, audio or other images of an identifiable individual qualifies as "personal information" under the *Acts.*

Since video surveillance systems can be operated to collect personal information about identifiable individuals, institutions must determine if they have the authority to collect this personal information in accordance with the *Acts.*

Pursuant to section 38(2) of the provincial *Act* and section 28(2) of the municipal *Act,* no person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

Institutions must be able to demonstrate that any proposed or existing collection of personal information by a video surveillance system is authorized under this provision of the *Acts.*

4. Considerations Prior to Using a Video Surveillance System

Before deciding to use video surveillance, it is recommended that institutions consider the following:

- A video surveillance system should only be considered after other measures of deterrence or detection have been considered and rejected as unworkable.

  Video surveillance should only be used where conventional means (i.e., foot patrols) for achieving the same law enforcement or public safety objectives are substantially less effective than surveillance or are not feasible, and the benefits of surveillance substantially outweigh the reduction of privacy inherent in collecting personal information using a video surveillance system.

- The use of **each** video surveillance camera should be justified on the basis of verifiable, specific reports of incidents of crime or significant safety concerns.

- An assessment should be conducted of the effects that the proposed video surveillance system may have on personal privacy, and the ways in which any adverse effects can be mitigated. Institutions may wish to refer to the Ontario Government's Privacy Impact Assessment tool.[1]

- Consultations should be conducted with relevant stakeholders as to the necessity of the proposed video surveillance program and its acceptability to the public. Extensive public consultation should take place.

- Institutions should ensure that the proposed design and operation of the video surveillance system minimizes privacy intrusion to that which is absolutely necessary to achieve its required, lawful goals.

[1] This document is available at <www.gov.on.ca/mbs/english/fip/pia>.

5. Developing the Policy for a Video Surveillance System

Once a decision has been made to use a video surveillance system, an institution should develop and implement a comprehensive written policy for the operation of the system. This policy should include:

- The rationale and objectives for implementing the video surveillance system.
- The use of the system's equipment, including: the location of the reception equipment; which personnel are authorized to operate the system, and the times when video surveillance will be in effect.
- The institution's obligations with respect to the notice, access, use, disclosure, retention, security and disposal of records in accordance with the *Acts.* (See Section 7.)
- The designation of a senior staff member to be responsible for the institution's privacy obligations under the *Acts* and its policy.
- A requirement that the institution will maintain control of and responsibility for the video surveillance system at all times.
- A requirement that any agreements between the institution and service providers state that the records dealt with or created while delivering a video surveillance program are under the institution's control and subject to the *Acts.*
- A requirement that employees and service providers review and comply with the policy and the *Acts* in performing their duties and functions related to the operation of the video surveillance system.

  Employees should be subject to discipline if they breach the policy or the provisions of the *Acts* or other relevant statutes. Where a service provider 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 of institutions and employees of service providers should sign written agreements regarding their duties under the policy and the *Acts,* including an undertaking of confidentiality.
- A requirement that there is a process in place to appropriately respond to any inadvertent disclosures of personal information.[2]

[2] See *A Privacy Breach Has Occurred - What Happens Next?* Presented by staff of the Information and Privacy Commissioner/Ontario at the Open Government 2001 - Access & Privacy Workshop. September 14, 2001. Available at <www.ipc.on.ca>.

- The incorporation of the policy into training and orientation programs of an institution and service provider. Training programs addressing staff obligations under the *Act* should be conducted on a regular basis.

- The policy should be reviewed and updated regularly at least once every two years.

6. Designing and Installing Video Surveillance Equipment

In designing a video surveillance system and installing equipment, the institution should consider the following:

- Reception equipment such as video cameras, or audio or other devices should only be installed in identified public areas where video surveillance is a necessary and viable detection or deterrence activity.

- The equipment should be installed in such a way that it only monitors those spaces that have been identified as requiring video surveillance. Cameras should not be directed to look through the windows of adjacent buildings.

- If cameras are adjustable by operators, this should be restricted, if possible, so that operators cannot adjust or manipulate them to overlook spaces that are not intended to be covered by the video surveillance program.

- Equipment should never monitor the inside of areas where the public and employees have a higher expectation of privacy (e.g., change rooms and washrooms).

- The institution should consider restricting video surveillance to periods when there is demonstrably a 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 the video surveillance areas, of video surveillance equipment locations, so the public has reasonable and adequate warning that surveillance is or may be in operation before entering any area under video surveillance. As a minimum requirement, signs at the perimeter of the surveillance areas should identify someone who can answer questions about the video surveillance system and include an address and telephone number for contact purposes.

- In addition, notification requirements under section 39(2) of the provincial *Act* and section 29(2) of the municipal *Act* include informing individuals of the legal authority for the collection of personal information; the principal purpose(s) for which the personal information is intended to be used and the title, business address and telephone number of someone who can answer questions about the collection. This information can be provided at the location on signage and/or by other means of public notification such as pamphlets. (Minimal requirements for signage are noted in the preceding paragraph.)

- Institutions should be as open as possible about the video surveillance program in operation and upon request, should make available to the public information on the rationale for the video surveillance program, its objectives and the policies and procedures that have been put in place. This may be done in pamphlet or leaflet form. A description of the program on an institution's website might also be an effective way of disseminating this information.

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

7. Access, Use, Disclosure, Retention, Security and Disposal of Video Surveillance Records

Any information obtained by way of video surveillance systems may only be used for the purposes of the stated rationale and objectives set out to protect public safety or to detect and deter criminal activity. Information should not be retained or used for any other purposes.

If the video surveillance system creates a record by recording personal information, the following policies and procedures should be implemented by the institution and should be included in the institution's policy discussed under Section 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. Each storage device that has been used should be dated and labeled with a unique, sequential number or other verifiable symbol.

- 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 to enable a proper audit trail.

- The institution should develop written policies on the use and retention of recorded information that:

  - Clearly state who can view the information and under what circumstances (i.e., because an incident has been reported, or to investigate a potential crime).

  - Set out the retention period for information that has not been viewed for law enforcement or public safety purposes. Recorded information that has not been used in this fashion should be routinely erased according to a standard schedule (normally between 48 and 72 hours).

  - Establish a separate retention period when recorded information has been viewed for law enforcement or public safety purposes. If personal information is used for this purpose, section 5 (1) of Ontario Regulation 460 under the provincial *Act* requires the recorded information to be retained for one year. Although section 5 of Ontario Regulation 823 under the municipal *Act* contains this provision, a resolution or by-law may reduce retention periods.

    Municipal institutions should consider passing a by-law or resolution, as contemplated by section 5 of Ontario Regulation 823, that makes their retention schedules explicit.

- The institution should store and retain storage devices required for evidentiary purposes according to standard procedures until the 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. This activity should be regularly monitored and strictly enforced.

- Old storage devices must be securely disposed of in such a way that the personal information cannot be reconstructed or retrieved. Disposal methods could include shredding, burning or magnetically erasing the personal information.

- An individual whose personal information has been collected by a video surveillance system has a right of access to his or her personal information under section 47 of the provincial *Act* and section 36 of the municipal *Act.* Policies and procedures must recognize this right. Access may be granted to one's own personal information in whole or in part, unless an exemption applies under section 49 of the provincial *Act* or section 38 of the municipal *Act.* Access to an individual's own personal information in these circumstances may also depend upon whether any exempt information can be reasonably severed from the record.

8. Auditing and Evaluating the Use of a Video Surveillance System

Institutions should ensure that the use and security of video surveillance equipment is subject to regular audits. The audit should also address the institution's compliance with the operational policies and procedures. An external body may be retained in order to perform the audit. Any deficiencies or concerns identified by the audit must be addressed immediately.

Employees and service providers should be aware that their activities are subject to audit and that they may be called upon to justify their surveillance interest in any given individual.

The institution should regularly review and evaluate its video surveillance program to ascertain whether it is still justified in accordance with the requirements in Section 4. This evaluation should occur at least once a year.

9. Other Resources

The personal information recorded by an institution's video surveillance system, and the institution's policies and practices respecting the personal information, are subject to the privacy protection provisions of the *Acts.*

Prior to implementing a video surveillance system or, for that matter, any new program with privacy implications, institutions should seek legal advice and consult with their Freedom of Information and Protection of Privacy Co-ordinator. Management Board Secretariat's Information and Privacy Office is a useful resource for Co-ordinators.

The Information and Privacy Commissioner/Ontario monitors compliance with the privacy protection provisions of the *Acts.* If an institution intends to introduce, significantly modify or expand a video surveillance system, they should consult with the Office of the Information and Privacy Commissioner/Ontario.

Appendix A — Covert Surveillance

Covert surveillance refers to surveillance conducted by means of hidden devices and should only be used as an absolute last resort. Prior to deciding to use covert surveillance for a purpose other than a case-specific law enforcement activity institutions should conduct a comprehensive assessment of the privacy impacts associated with the implementation of such a program. Institutions should submit this assessment, together with the case for implementing covert surveillance, to the Office of the Information and Privacy Commissioner/ Ontario. See Section 9 for additional resources.

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

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