Information
and Privacy
Commissioner/
Ontario

Guidelines for the Use of Video Surveillance Cameras in Public Places

Ann Cavoukian, Ph.D.
Commissioner
September 2007

Acknowledgements

This publication is an updated version of a paper released in 2001 by Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario. Dr. Cavoukian gratefully acknowledges the work of Judith Hoffman in preparing the first report, and Catherine Thompson for her work on this updated report.

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

Organizations 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 are encouraged not to view video surveillance as a "silver bullet." Although technological solutions to security challenges reflect an "urge for perfect fairness and perfect security, extended equally and automatically to all,"[1] no such world of perfection exists. Institutions must balance the public benefits of video surveillance 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 organizations 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 covert surveillance, or 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.

These *Guidelines* are also not intended to apply to workplace surveillance systems installed by an organization to conduct workplace surveillance of employees.

[1] See Jeffrey Rosen, *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age* (Toronto: Random House, 2004), page 123. Also, see generally *The Naked Crowd*, Chapter Three "The Silver Bullet."

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, digital or wireless[2] 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.

[2] See *Wireless Communication Technologies: Video Surveillance Systems (Fact Sheet)* available on the Office of the Information and Privacy Commissioner of Ontario's website (www.ipc.on.ca).

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*.[3]

Since video surveillance systems can be operated to collect personal information about identifiable individuals, organizations 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 organization 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. For example, the collection of personal information that is merely helpful and not necessary to the proper administration of a lawfully authorized activity would not meet the requirements of sections 28(2) and 38(2).[4]

Organizations 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*.

[3] Note, our Office has held that under the *Personal Health Information Protection Act,* a record is created when a camera and transmitter capture an image, and encode and wirelessly transmit that image, even if a physical artifact is not created such as a videotape or CD containing the image. See Order HO-005 available on the Office of the Information and Privacy Commissioner of Ontario's website (www.ipc.on.ca).

[4] *Cash Converters Canada Inc. v. Oshawa* (City) [2007] O.J. No. 2613, at 40.

4. Considerations Prior to Using a Video Surveillance System

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

- A video surveillance system should only be considered after other measures to protect public safety, detect or deter, or assist in the investigation of criminal activity have been considered and rejected as unworkable.

  Video surveillance should only be used where conventional means (e.g., 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 of privacy implications 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 by examining the collection, use, disclosure and retention of personal information. Organizations may wish to refer to the Ontario Government's Privacy Impact Assessment tool.[5]

- 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.

- Organizations 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.

[5] This document is available at http://www.accessandprivacy.gov.on.ca/english/pub/screeningtool.html

5. Developing the Policy for a Video Surveillance System

Once a decision has been made to use a video surveillance system, an organization 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 access the storage device, and the times when video surveillance will be in effect.
- The organization'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 organization's privacy obligations under the *Acts* and its policy.
- A requirement that the organization will maintain control of and responsibility for the video surveillance system at all times.
- A requirement that any agreements between the organization and service providers state that the records dealt with or created while delivering a video surveillance program are under the organization'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 relating 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 should be considered a breach of contract leading to penalties up to and including contract termination.

  Employees of organizations 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 privacy breaches.[6]

- The incorporation of the policy into all training and orientation programs of an organization 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 every two years or sooner if there is a change or upgrade to the video surveillance system.

6. Designing and Installing Video Surveillance Equipment

In designing a video surveillance system and installing the necessary equipment, the organization 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 necessary to protect public safety, detect or deter, and assist in the investigation of criminal 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, zoom or manipulate the camera to overlook spaces that are not intended to be covered by the video surveillance program.

- Equipment should not monitor the inside of areas where individuals generally have a higher expectation of privacy (e.g., change rooms and public washrooms).

- The organization should consider restricting video surveillance to time periods when there is a demonstrably higher likelihood of crime being committed and detected in the area under surveillance.

[6] A privacy breach occurs when personal information is collected, retained, used or disclosed in ways that are not in accordance with the provisions of the *Acts*. See publications available on the Office of the Information and Privacy Commissioner of Ontario's website (www.ipc.on.ca) such as the *Breach Notification Assessment Tool*, and *What to do if a privacy breach occurs: Guidelines for government organizations*.

- 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. Signs at the perimeter of the surveillance areas should identify someone who can answer questions about the video surveillance system, and can include an address, telephone number, or website 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 or the organization's website. See Appendix A for a good example of a city's sign.

- Organizations 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 organization's website would 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 organization's policy, should have access to the controlled access area and the reception equipment. Video monitors should never 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, detect or deter, and assist in investigating criminal activity. Information should not be retained or used for any other purposes.

Where records of personal information created using video surveillance are to be retained, the following policies and procedures should be implemented by the organization and should be included in the organization'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 made by authorized personnel. Logs should be kept of all instances of access to, and use of, recorded material, to enable a proper audit trail. Electronic logs should be kept where records are maintained electronically.

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

    - Clearly state who can view the information and under what circumstances (e.g. where 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). For example, images are not monitored from a video surveillance system in Toronto's entertainment district introduced in 2007. Images are overridden automatically every 72 hours and are not accessed unless an incident prompts an investigation.

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

- The organization should store and retain storage devices required for evidentiary purposes in accordance with their own policies 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, and 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 overwriting electronic records, shredding, burning or magnetically erasing the personal information. See *Secure Destruction of Personal Information (Fact Sheet)* available on the Office of the Information and Privacy Commissioner of Ontario's website (www.ipc.on.ca).

- 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*. All 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*, such as where disclosure would constitute an unjustified invasion of another individual's privacy. 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. One way in which this may be achieved is through digitally "blacking out" the images of other individuals whose images appear on the videotapes.

Video surveillance systems using wireless technology must securely encrypt the wireless transmission of all personal information. See *Wireless Communication Technologies: Safeguarding Privacy & Security (Fact Sheet)* available on the Office of the Information and Privacy Commissioner of Ontario's website (www.ipc.on.ca).

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

Organizations should ensure that the use and security of video surveillance equipment is subject to regular audits. The audit should also address the organization'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 organization 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 organization's video surveillance system, and the organization'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, organizations should seek legal advice and consult with their Freedom of Information and Protection of Privacy Co-ordinator. The Ministry of Government Service's Access and Privacy Office is a useful resource for Co-ordinators.

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

Organizations should also consult the publications available on the Office of the Information and Privacy Commissioner of Ontario's website (www.ipc.on.ca), such as:

- Wireless Communication Technologies: Safeguarding Privacy & Security (Fact Sheet)
- Wireless Communication Technologies: Video Surveillance Systems (Fact Sheet)
- Secure Destruction of Personal Information (Fact Sheet)
- Breach Notification Assessment Tool
- What to do if a Privacy Breach Occurs: Guidelines for Government Organizations

Appendix A – Example of a city's sign

Attention

This Area May Be Monitored by Video Surveillance Cameras (CCTV)

The personal information collected by the use of the CCTV at this site is collected under the authority of (an Act) and (by-law). This information is used for the purpose of promoting public safety and reduction of crime at this site.

Any questions about this collection can be directed to the Manager of (Department) at (phone number), (City Hall address) (e-mail).