VIDEO SURVEILLANCE GUIDELINES

Introduction

Surveillance of public spaces has increased rapidly over recent years. This growth is largely attributed to the significant advances in surveillance technology and its growing affordability, as well as the perception that video surveillance increases public safety and security.

Although there is some debate regarding the deterrent effect of video surveillance technology on crime, it nevertheless remains the most common reason why public bodies and trustees (organizations) consider using surveillance systems. Regardless of the reason for using a surveillance system, it is important to recognize that cameras capture a great deal more than crimes in the making – including responsible citizens going about their daily lives. And while collection of this information may appear harmless, there are laws regarding individual privacy rights and responsibilities that organizations must adhere to.

The pervasive surveillance of ordinary, lawful activities can significantly interfere with an individual's right to privacy. Accordingly, organizations that are considering implementing a surveillance system must balance the benefits of surveillance against individual privacy rights in a democratic society.

Purpose and scope

As the use of surveillance become more prevalent in Manitoba, our office acknowledges the need for guidance when organizations consider using surveillance systems. Implementing a surveillance system requires careful consideration and forethought to minimize the impact on the privacy rights of individuals.

In Manitoba, *The Freedom of Information and Protection of Privacy Act* (FIPPA) and *The Personal Health Information Act* (PHIA) recognize and protect an individual's privacy rights. FIPPA and PHIA govern the collection, use and disclosure of personal and personal health information held by organizations.

These guidelines aim to assist organizations in deciding whether a proposed or existing surveillance system is operating in a privacy protective manner.

For the purposes of these guidelines, we are dealing only with surveillance conducted by public bodies and trustees in open, public spaces, in public buildings, and on public transportation. These guidelines do not apply to covert surveillance being used as a case-specific investigation tool for law enforcement purposes.

Private-sector organizations in Manitoba are governed by federal legislation, the *Personal Information Protection and Electronic Documents Act* (PIPEDA). PIPEDA sets out the ground rules for how private-sector organizations such as businesses collect, use or disclose personal information in the course of commercial activities.

While our guidelines address surveillance in the public sector, many of the best practices are consistent with the surveillance guidelines for the private sector developed by the Office of the Privacy Commissioner of Canada and may be beneficial for Manitoba businesses who are contemplating a surveillance system. For specific information about overt and covert video surveillance in the private sector, please refer to the Office of the Privacy Commissioner of Canada website:

Private Sector Covert Surveillance:
https://www.priv.gc.ca/information/pub/gd_cvs_20090527_e.asp

Private Sector Overt Surveillance:
https://www.priv.gc.ca/information/guide/2008/gl_vs_080306_e.asp

Manitoba Ombudsman
www.ombudsman.mb.ca | ombudsman@ombudsman.mb.ca | 1-800-665-0531 | 204-982-9130

CONSIDERING USING SURVEILLANCE?

Manitoba Ombudsman's Top 10 Considerations

1 Justifying surveillance and evaluating less privacy-intrusive options

The use of a surveillance system must be justified on the basis of verifiable safety concerns or other demonstrable circumstances (for example, specific reports of incidents of crime).

Organizations need to determine whether there are other measures to protect public safety or to deter or detect crime that would be reasonable and less privacy-intrusive. Video and/or audio surveillance should always be considered a last resort.

If surveillance is considered, organizations should evaluate the potential impact surveillance would have on individual privacy. The organization should also establish whether the surveillance is permitted under FIPPA and PHIA.

2 Collection of personal and personal health information

Under FIPPA and PHIA, any recording of personal or personal health information constitutes a collection of that information. Organizations must determine if they have the authority to collect the information in accordance with the applicable legislation before they consider a surveillance system.

In addition, every component of the surveillance system must be permitted by the applicable legislation. For example, if an organization is considering the implementation of a surveillance system that collects video and audio footage, they must be able to demonstrate the purpose and the legal authority for the collection of both types of footage. This should include evidence that supports how each component fulfils the purpose for the collection. If the organization cannot identify provisions within the applicable legislation that authorizes the collection, the surveillance system should not be considered further.

For more specific information regarding the collection of personal and personal health information, please refer to Manitoba Ombudsman's practice notes titled *Collection and Providing Notice of Collection of Personal Information under FIPPA* and *Collection and Providing Notice of Collection of Personal Health Information under PHIA* on the Manitoba Ombudsman's website at www.ombudsman.mb.ca.

3 Developing a surveillance system policy

If an organization decides to implement a surveillance system, a written policy should be developed which clearly outlines the following:

- the rationale and objectives for implementing the surveillance system
- the legislative authority under FIPPA or PHIA for the collection of personal or personal health information
- the use of the system's equipment, including:
    - the location of the equipment,
    - the personnel authorized to operate the system

    - the personnel authorized to operate and or access the storage device
    - and the times when surveillance will be in effect
- information that will be shared with the public about the surveillance system such as the personal information captured, the collection, use, disclosure, retention, destruction, security and access of the personal and personal health information
- the designation of a senior staff member responsible for the organization's privacy obligations under the act(s) and its policy, including name, title and phone number
- direction as to who is permitted to view the records, video or audio data and under what circumstances, for example, an incident has been reported or suspected
- a requirement that the organization will maintain control of and responsibility for the surveillance system at all times
- a requirement that any agreement between the organization and a contractor state that the records created while delivering the surveillance program are under the organization's control and subject to FIPPA and/or PHIA as applicable
- a requirement that employees and contractors review and comply with the policy and the act(s) in performing their duties and functions relating to the operation of the surveillance system and that they sign written agreements regarding their responsibilities under the policy and the act(s), including an undertaking of a pledge of confidentiality (as required by PHIA)
- a requirement that there is a process in place to respond appropriately to any privacy breach (see the practice notes titled *Key Steps in Responding to Privacy Breaches under The Freedom of Information and Protection of Privacy Act (FIPPA) and The Personal Health Information Act (PHIA)* and *Reporting a Privacy Breach to Manitoba Ombudsman* on the Manitoba Ombudsman's website at www.ombudsman.mb.ca)
- the incorporation of the policy, including staff and contractor obligations, into regular training and orientation programs
- a review of and update to the policy every two years or sooner if changes or upgrades are made to the surveillance system

4 Design and implementation of a surveillance system

When designing a surveillance system, the following should be kept in mind:

- A surveillance system should only be installed in identified public areas where surveillance is a necessary and a viable means of deterring or detecting crime or protecting public safety.
- The equipment should be installed in such a way that it only monitors those spaces that have been identified as requiring surveillance.
- 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 surveillance program.
- Equipment should not monitor the inside of areas where individuals generally have a higher expectation of privacy, for example, inside change rooms and washrooms.
- The use of surveillance should be restricted to time periods when there is a demonstrably higher likelihood of crime being committed and detected in the area under surveillance.
- Access to the surveillance system should be in a strictly controlled area. Only those who are authorized to use the system should have access to the controlled area and the surveillance equipment. Video monitors should never be in a position that enables public viewing.

5 Notifying the public

The public must be provided with reasonable and adequate notice that surveillance is or may be in operation.

An organization should be as open as possible about its surveillance program and should be prepared to share information with the public about the rationale for the surveillance. This would include describing the purpose of conducting surveillance, the legal authority permitting the surveillance and the contact information of the organization's employee who can answer any questions regarding the surveillance. Providing reasonable and adequate notice may be achieved by clearly and prominently displaying a sign or poster at the perimeter of surveillance areas.

6 Using and disclosing surveillance records

Information collected through video and/or audio surveillance should not be used or disclosed beyond the initial identified purpose unless it is otherwise authorized by legislation. The practice of collecting personal information for one reason and then later using the collected information for a different reason is referred to by privacy professionals as "function creep." Function creep is problematic because it can lead to organizations using personal information in ways that do not meet the requirements of FIPPA or PHIA. For example, if an organization uses video surveillance at an entry to a building for law enforcement purposes and later wants to use the information to track employee attendance, the organization must first determine whether the applicable legislation authorizes the new use of the collected information. Otherwise the new use of the information may be unlawful.

Organizations must also limit the use of personal and personal health information to only those employees who need to know the information to accomplish the initial purpose of the collection. Also, every disclosure of personal information must be limited to the minimum amount of information necessary to accomplish the purpose.

Logs should be kept identifying when the surveillance records were utilized, by whom, and for what purpose. Additionally, logs should be kept of all instances of disclosure of the surveillance records, indicating the specific information disclosed, to whom it was disclosed, the date of the disclosure and the purpose for the disclosure.

7 Retention and destruction of surveillance records

An organization should prepare a retention and destruction schedule to specify the length of time that surveillance records will be kept, when records will be destroyed, and how the records will be destroyed. A schedule should be based on a time period in which a suspected or actual incident could be revealed. If no suspected or actual incidents are revealed within that established time period, the information recorded during that time could be routinely erased or overridden. A retention period should also be established for information that reveals actual incidents; the time period should allow for appropriate action(s) to be taken in response to the information recorded, but not longer.

Again, the organization should determine how surveillance records will be destroyed once a retention period has passed.

8 Security of surveillance records

All storage devices must be securely stored when not in use. For example, secure storage may include password protection of a digital device that is in a locked receptacle located in a controlled-access area. All storage devices that have been used should be numbered and dated.

Storage devices that may be required for evidentiary purposes should be retained in accordance with policies until requested by law enforcement authorities. A storage device release form should be completed before any storage device is disclosed. The form should indicate:

- who took the device
- time and date the device was taken
- the legislative provision that permitted the disclosure of the device
- the legislative provision that permitted the collection of the device
- if the device will be returned or destroyed after use.

All disclosures of storage devices should be regularly monitored and compliance with the surveillance system policy strictly enforced.

If wireless technology is being used, the organization must securely encrypt the wireless transmission of all personal or personal health information. An information technology specialist should be involved with the transmission to ensure appropriate technological measures are taken.

9 Access to surveillance records

Individuals have the legal right to access their personal and personal health information. This right also extends to surveillance records. Access may be granted to general information, to personal or personal health information in whole or in part, unless an exception applies under FIPPA or PHIA.

Access to surveillance records may also depend on whether information that cannot legally be disclosed to an individual can reasonably be removed from the record. It may be possible to digitally black out or blur the images of other individuals in the footage, for example.

10 Auditing surveillance systems

Organizations should ensure that the use and security of surveillance equipment including cameras, monitors and storage devices is periodically audited and compliant with operational policies and procedures. The audit should also address employees' compliance with FIPPA or PHIA and any related policies and procedures. The results of each audit should be documented and any deficiencies or concerns identified by the audit should be addressed.

Employees and contractors using the system should be aware that their activities are subject to audit. An audit clause should be added to any contract for the provision of surveillance services. Organizations should regularly review and evaluate surveillance systems to determine whether surveillance continues to be required or justified.

Conclusion

Manitoba Ombudsman oversees compliance with *The Freedom of Information and Protection of Privacy Act* and *The Personal Health Information Act* by conducting investigations and reviewing privacy and access practices. The ombudsman investigates, monitors and audits compliance with the privacy protection provisions of FIPPA and PHIA. Manitoba Ombudsman may be consulted for advice or guidance regarding the potential use of a surveillance system or any significant modification or expansion of a surveillance system.

Organizations should also consider seeking legal advice and consulting with their access and privacy coordinator or privacy officer before implementing a surveillance system. While it is not mandatory, a privacy impact assessment is considered a best practice and is a very useful tool to help clarify any issues prior to designing and installing a surveillance system.

Because the use of video and audio surveillance is very intrusive to individual privacy rights and raises

a number of controversial issues, organizations need to assess the true need and value of video surveillance. The organization must balance the benefits of using surveillance technology with the potential cost to individual privacy.

ACKNOWLEDGMENTS

We gratefully acknowledge the contributions of the Office of the Privacy Commissioner of Canada and the Information and Privacy Commissioner's offices in British Columbia, Alberta, Saskatchewan, Ontario, Newfoundland and Labrador to our Video Surveillance Guidelines. Our guidelines incorporate much of their collective advice and knowledge.

Manitoba Ombudsman
750 - 500 Portage Avenue
Winnipeg, MB R3C 3X1

204-982-9130 (phone)
1-800-665-0531 (toll-free in Manitoba)
204-942-7803 (fax)
ombudsman@ombudsman.mb.ca (general email inquiries)

www.ombudsman.mb.ca
www.facebook.com/manitobaombudsman

February 2015