FEDERAL

Privacy Commissioner of Canada

PROVINCIAL

Information and Privacy Commissioner of Alberta

Information and Privacy Commissioner for British Columbia

Guidelines for Overt Video Surveillance in the Private Sector

March 2008

Introduction

The use of video surveillance by private sector organizations has exploded in recent years. As technology has evolved and costs have fallen dramatically, video surveillance is increasingly accessible to a large range of organizations. Security and crime control concerns are the most common motivating factors for the deployment of video surveillance cameras. Retailers use cameras in hopes of deterring thefts and identifying suspects. Cameras are installed in apartment buildings to detect vandalism and increase the security of tenants. But there are other less obvious uses as well. Some retailers conduct video surveillance to analyze consumer behaviour – which store aisles they frequent, where they stop, what products they examine.

Private sector privacy laws require that organizations' need to conduct video surveillance must be balanced with the individuals' right to privacy, which includes the right lead their lives free from scrutiny. Given its inherent intrusiveness, organizations should consider all less privacy-invasive means of achieving the same end before resorting to video surveillance.

To help organizations achieve compliance with private sector privacy legislation, we have developed these Guidelines, which set out the principles for evaluating the use of video surveillance and for ensuring that its impact on privacy is minimized. These Guidelines apply to overt video surveillance of the public by private sector organizations in publicly accessible areas. These Guidelines *do not* apply to covert video surveillance, such as that conducted by private investigators on behalf of insurance companies, nor do they apply to the surveillance of employees.

An important note – private sector privacy laws[1] govern the collection, use and disclosure of information about an identifiable individual. In the private sector, surveillance through a video camera is subject to privacy laws. Under PIPEDA and the Alberta and British Columbia *PIPA*s, the information does not need to be recorded.

[1] *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)
Alberta's *Personal Information Protection Act* (*PIPA*)
British Columbia's *Personal Information Protection Act* (*PIPA*)
Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector*

10 things to do when considering, planning and using video surveillance

1. Determine whether a less privacy-invasive alternative to video surveillance would meet your needs.

2. Establish the business reason for conducting video surveillance and use video surveillance only for that reason.

3. Develop a policy on the use of video surveillance.

4. Limit the use and viewing range of cameras as much as possible.

5. Inform the public that video surveillance is taking place.

6. Store any recorded images in a secure location, with limited access, and destroy them when they are no longer required for business purposes.

7. Be ready to answer questions from the public. Individuals have the right to know who is watching them and why, what information is being captured, and what is being done with recorded images.

8. Give individuals access to information about themselves. This includes video images.

9. Educate camera operators on the obligation to protect the privacy of individuals.

10. Periodically evaluate the need for video surveillance.

Qs and As

Q. What can we use video surveillance for?

A. There are a number of situations where it may be reasonable to expect video surveillance to take place, for example, for security purposes around banking machines or inside convenience stores in high-crime areas. In areas where people have a much higher expectation of privacy, such as a public washroom or a spa treatment room, video surveillance is inappropriate.

When considering the use of video surveillance, make sure that all less privacy invasive alternatives have been looked at. It is preferable to first put the appropriate security measures in place, such as placing inventory under lock and key.

Q. What are we allowed to do with the information we obtain through video surveillance?

A. Information collected through video surveillance should only be used for the purpose that surveillance is being undertaken, or for purposes that are permitted by law. For example, if cameras are installed in an apartment building parking garage for safety purposes, the information cannot be used to track the movements of tenants. However, if a car is broken into, the information can be disclosed to law enforcement.

Q. What should we keep in mind when installing and operating the cameras?

A. The video surveillance system should be set up and operated to collect the minimum amount of information to be effective. This helps reduce the intrusion on individuals' privacy. Specifically:

- Cameras that are turned on for limited periods in the day are preferable to "always on" surveillance.
- Cameras should be positioned to reduce capturing images of individuals who are not being targeted. For example, a store security camera should not be recording passersby outside the store.
- Cameras should not be aimed at areas where people have a heightened expectation of privacy, for example, showers or into windows. Steps should be taken to ensure that cameras cannot be adjusted or manipulated by the operator to capture images in such areas.
- Sound should not be recorded unless there is a specific need to do so.
- If a camera is monitored, the recording function should be turned on only when unlawful activity is suspected or observed.

Organizations should also ensure that the video surveillance complies with all applicable laws, in addition to privacy legislation. For example, an organization using a video camera that captures sound needs to consider the *Criminal Code* provisions dealing with the collection of private communications.

Q. Should we post signs that there are cameras in operation?

A. Yes. Most privacy laws require the organization conducting video surveillance to post a clear and understandable notice about the use of cameras on its premises to individuals whose images might be captured by them, *before* these individuals enter the premises. This gives people the option of not entering the premises if they object to the surveillance. Signs should include a contact in case individuals have questions or if they want access to images related to them.

Q. What are our responsibilities with regard to recorded images?

A.

- The recorded images must be stored in a secure location, and access should be granted only to a limited number of authorized individuals.
- Individuals have the right to access images relating to them. When disclosing recordings to individuals who appear in them, the organization must ensure that identifying information about any other individuals on the recording is not revealed. This can be done through technologies that mask identity.
- Any disclosure of video surveillance recordings outside the organization should be justified and documented.
- Recordings should only be kept as long as necessary to fulfill the purpose of the video surveillance. Recordings no longer required should be destroyed. Organizations must ensure that the destruction is secure.

Q. What are our obligations to the people who operate our video surveillance system?

A. Organizations should ensure that appropriate and ongoing training is provided to operators to make certain that they:

- understand their obligations under all relevant legislation, these Guidelines, and the organization's video surveillance policy; and
- conduct surveillance only for the purposes identified by the organization.

Q. Once the video surveillance system is up and running, what do we need to do to ensure continued compliance with privacy laws?

A. Organizations should evaluate all aspects of the operation of their video surveillance system regularly. In particular, organizations should examine whether video surveillance continues to be required and should consider:

- Was video surveillance effective in addressing the problem for which it was introduced?
- Does the problem still exist?
- Would a less intrusive way of addressing the problem now be effective?

Q. How should my organization document the use of video surveillance?

A. Organizations should develop a policy on video surveillance that sets out:

- the rationale and purpose of the surveillance system;
- the location and field of vision of the equipment;
- any special capabilities of the system, for example, sound, zoom, facial recognition or night-vision features;
- the rationale and purpose of the specific locations of equipment and fields of vision selected;
- the personnel authorized to operate the system and access the information it contains;
- the times when surveillance will be in effect;
- whether and when recording will occur;
- the place where signals from the equipment will be received and monitored;
- guidelines for managing video surveillance recordings, including security, use, disclosure, and retention;
- procedures for the secure disposal of video surveillance recordings;
- a process to follow if there is unauthorized disclosure of images;
- procedures for individuals to access personal information captured and challenge any suspected failure to comply with the policy;
- sanctions for the organization's employees and contractors for failing to adhere to the policy; and
- the individual accountable for privacy compliance and who can answer any questions about the surveillance.