Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Technology Fact Sheet

Video Surveillance

November 2016

INTRODUCTION

This fact sheet provides institutions subject to the *Freedom of Information and Protection of Privacy Act* or the *Municipal Freedom of Information and Protection of Privacy Act* (*FIPPA*, *MFIPPA* or the acts) with basic information about how to use video surveillance in a way that protects individual privacy. More detailed guidance can be found in the IPC's **Guidelines for the Use of Video Surveillance**.

DOES YOUR INSTITUTION HAVE THE AUTHORITY TO INSTALL A VIDEO SURVEILLANCE SYSTEM?

Institutions can collect personal information through the use of a video surveillance system if the collection is authorized under *MFIPPA* or *FIPPA*. Video surveillance may be authorized in cases where the system is used for the purposes of law enforcement, for example the use of temporary cameras by police for planned protests. It may also be authorized when necessary for the administration of your institution's lawful activities.

Video surveillance may be considered *necessary* if:

- the goals or purposes of the collection cannot be achieved by less privacy intrusive means, and
- the surveillance is more than merely helpful

For instance, circumstances may justify a school board's or a public transit authority's use of video surveillance to ensure safety on school property or on buses and subway systems.

ARE THERE LIMITS TO THE NUMBER AND PLACEMENT OF CAMERAS?

Yes. The video surveillance system should use as few cameras as possible. Cameras should be placed only in those locations where they are needed.

You should ensure that:

- the number of cameras and their placement captures the *least* amount of personal information necessary to achieve the purposes of the program – do not collect more personal information than you need
- the cameras are not in areas where individuals have a high expectation of privacy, such as washrooms
- any pan and zoom functions are disabled, or their use is minimized to prevent over collection

SHOULD YOUR INSTITUTION CONDUCT CONSULTATIONS?

Yes. Identify and consult with individuals who will be affected by the video surveillance. Both internal and external stakeholders should be involved, including legal or privacy experts in your organization, such as the freedom of information coordinator. For example, school boards should engage with teachers, students, families and local residents before installing video surveillance on school property.

IS YOUR INSTITUTION REQUIRED TO NOTIFY INDIVIDUALS THAT VIDEO SURVEILLANCE IS TAKING PLACE?

Yes, notification of video surveillance is required. Post notices at every video surveillance location and on your website. Notices should use plain language with graphics that can be easily understood.

Notices should either explain or direct individuals to a source explaining:

- the legal authority for collection
- how the personal information will be used
- the title, business mailing or email address and business telephone number of a public official who can answer questions about the video surveillance program

HOW CAN YOUR INSTITUTION USE THE INFORMATION COLLECTED?

Privacy laws prohibit the use of personal information except in specific circumstances.

As a general rule, you should not use video unless:

- the reason for its use is the same or consistent with the purpose of the video surveillance system, or
- you have the consent of the individual whose personal information appears in the video

Limit the number of people who have access to the images by clearly defining who should have access, in what circumstances and for what purpose. For example, if the purpose is to deter and identify individuals involved in crime or vandalism, only allow access to the

images related to these specific incidents and limit the number of individuals in your organization who can access them.

CAN YOUR INSTITUTION DISCLOSE VIDEO IMAGES?

The acts also prohibit the disclosure of personal information except in specific circumstances. Ensure that your institution's disclosure policies and practices are consistent with the acts. Circumstances where you may disclose video images include:

- when you have the consent of the individuals whose personal information appears in the images
- when responding to an access request under the acts
- when it is requested by the police – with or without a warrant – to aid an investigation

HOW LONG CAN YOUR INSTITUTION KEEP THE IMAGES?

If video images have not been used or disclosed, your institution should routinely delete them at the earliest opportunity. For example, if your office is closed over a weekend you may not discover that an incident has occurred until the next business day. In this case, the images may need to be retained for enough time to allow them to be reviewed when the office reopens.

If an institution uses or discloses the images for any purpose:

- institutions subject to *FIPPA* are required to retain the images for one year after use
- institutions subject to *MFIPPA* are required to retain the images for one year after use or as required by applicable by-laws, whichever is shorter

WHAT SECURITY MEASURES SHOULD YOUR INSTITUTION HAVE IN PLACE?

Institutions must have reasonable methods to ensure the images captured by video surveillance are secure. This means that the confidentiality, integrity and availability of the images must be protected. This includes steps for strict access controls based on the individual's role.

Security measures should include:

- administrative measures, such as the development of clear policies and procedures regarding use and disclosure
- technical measures, such as ensuring that images are encrypted and that robust controls are in place that ensure only those who need the information can access it (this includes logging and auditing)
- physical measures, such as ensuring secure locations for video monitors and image storage

ARE THERE OTHER CONSIDERATIONS TO HELP ENSURE THAT THE PROGRAM IS COMPLIANT?

- Review and follow the IPC **Guidelines for the Use of Video Surveillance**
- Conduct a Privacy Impact Assessment and consult the IPC's **Planning for Success: Privacy Impact Assessment Guide**
- Develop clear policies and ensure that staff involved are adequately trained and aware of their responsibilities
- Ensure that the system includes processes to allow for information to be retrieved in the event that an individual requests access to the images