Video Surveillance Policy Template

Office of the Information and Privacy Commissioner

Forward

The Office of the Information and Privacy Commissioner for Nova Scotia (OIPC) has a public education mandate under the *Privacy Review Officer Act*. In combination with our recently updated *Guidelines for the Use of Video Surveillance in Nova Scotia* this document is intended to provide public bodies and municipalities with the information necessary to ensure that any use of video surveillance is in compliance with their privacy obligations set out in the *Freedom of Information and Protection of Privacy Act* (*FOIPOP*) and the *Municipal Government Act* (*MGA*).

Acknowledgments

The Office of the Information and Privacy Commissioner for Nova Scotia gratefully acknowledges that this guidance document is based in part on the work of:

- Office of the Information and Privacy Commissioner for Ontario, *Guidelines for the Use of Video Surveillance, October 2015* https://www.ipc.on.ca/wp-content/uploads/Resources/2015_Guidelines_Surveillance.pdf
- Office of the Information and Privacy Commissioner for British Columbia, *Guide to using overt video surveillance, December 2016* https://www.oipc.bc.ca/guidance-documents/2006
- Office of the Information and Privacy Commissioner for Newfoundland and Labrador, *OIPC Guidelines for Video Surveillance by Public Bodies in Newfoundland and Labrador, June 26, 2016* http://www.oipc.nl.ca/pdfs/GuidelinesForVideoSurveillance.pdf .
- Office of the Saskatchewan Information and Privacy Commissioner, *Video Surveillance Guidelines for Public Bodies, March 2016* http://www.oipc.sk.ca/Resources/2016-2017/Video%20Surveillance%20Guidelines.pdf
- Privacy Commissioner of New Zealand, *Privacy and CCTV: A guide to the Privacy Act for businesses, agencies and organizations, October 2009* https://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-and-CCTV-A-guide-October-2009.pdf

Introduction

Public bodies and municipalities in Nova Scotia are responsible for ensuring the safety of individuals and the security of the equipment and property within the scope of the services they provide. One tool used by many public bodies and municipalities to help them fulfill this obligation is video surveillance.

While video surveillance may help to increase the safety of individuals and the security of assets, it also introduces risks to the privacy of individuals whose personal information may be collected, used and disclosed as a result of the technology. The risk to privacy is particularly acute because video surveillance may, and often does, capture the personal information of law-abiding individuals going about their everyday activities. In view of the broad scope of personal information collected, special care must be taken when considering whether and how to use this technology.

Preliminary Steps

The *Guidelines for the Use of Video Surveillance in Nova Scotia* provide an explanation of the necessary considerations and steps to take before implementing video surveillance. It is available on our website at: www.foipop.ns.ca.

Policy Template

The *Guidelines for the Use of Video Surveillance in Nova Scotia* explain that one of the key documents you must complete before switching on your video surveillance system is a video surveillance policy. This policy will ensure that you have communicated the exact purposes and all of the rules regarding the collection, use, disclosure of personal information via video surveillance and the security of your video surveillance system.

A video surveillance policy should include the following sections:

1. Purpose
2. Collection
3. Notification
4. Use
5. Disclosure
6. Security
7. Retention
8. Access to Information Requests
9. Contact Information

1. Purpose

Describe the purposes for which video surveillance may be used by the public body or municipality. Include a detailed rationale for surveillance. Explain your rationale in a way that both staff and citizens will understand. Ensure that the purposes listed here are authorized under the *Freedom of Information and Protection of Privacy Act* (*FOIPOP*) or the *Municipal Government Act* (*MGA*). You will determine this by first completing a privacy impact assessment.[1]

[1] The Office of the Information and Privacy Commissioner has published privacy impact assessment templates on our website at: https://foipop.ns.ca/publicbodytools.

2. Collection

You should clearly state what personal information you intend to collect and what information you will not collect.

Identify the types of personal information that may be collected as part of the authorized video surveillance. For example, is the intention to only collect information of customers or citizens, or will the personal information of employees or service providers be collected as well?

Clearly describe the physical areas/locations where collection of personal information through video surveillance is authorized. State the limits on the location and field of vision of the equipment including the rationale and purpose of the specific locations of equipment and fields of vision selected.

Specify here prohibitions on the use of video surveillance in such areas as change rooms, washrooms, neighbouring properties including cameras pointed through neighbouring windows, etc.

Specify limitations on collection such as time of day, limits on location, field of vision, limits on any special capabilities of the system such as sound, zoom, facial recognition or night vision features.

3. Notification

Nova Scotia's access and privacy laws do not require that public bodies and municipalities provide notification when information is collected directly from citizens as it is with video surveillance. However, best privacy practice requires that proper notification be given to individuals. Such an approach respects the right of individuals to choose whether or not they wish to be subject to video surveillance. From a practical perspective, if the rationale for the surveillance is that the presence of video surveillance reduces the chance of illegal activity clear and prominent notifications are necessary. How can video surveillance reduce the chance of illegal activity if citizens are unaware of the surveillance?

In the policy you should describe the requirements for notification including the number of signs, locations and information to be included on authorized notices. Ideally, include a template notification sign in the appendix to your policy. See the OIPC guidelines for further details on the best practice content of video surveillance notifications.

4. Use

List all of the authorized uses of the video surveillance data. Clearly state any limitations on use. Generally speaking, best practice is to limit the use of the information to only those purposes for which it was originally collected. Any secondary use of the information must be subject to careful evaluation of the authority under *FOIPOP* or the *MGA*. For example, video surveillance conducted for security purposes cannot be used to monitor employee attendance or to monitor employee compliance with dress codes.

5. Disclosure

List all anticipated and authorized disclosures of personal information from the video surveillance data. This should include disclosures that are likely to occur based on experience. For example, if the purpose for the collection of the data is security, it is reasonable to anticipate that the public body or municipality may need to disclose video surveillance data to police as authorized under 27(l) of *FOIPOP* and s. 485(2)(l) of the *MGA*.

In addition, depending on the nature of the video surveillance undertaken, it may be reasonable to anticipate that a law enforcement agency may make a request for disclosure of video surveillance data through the use of a warrant (as authorized under s. 27(e) of *FOIPOP* and s. 485(2)(e) of the *MGA*).

Specify here the process the public body or municipality will use if it receives a request for disclosure of video surveillance data. Typically the process should include:

- identification of who within your organization is authorized to disclose the data,
- a requirement that the requester put his or her request in writing stating the authority he or she claims for the disclosure,
- a requirement that all disclosures be documented by including a copy of the request,
- a log of the information disclosed, and
- a clear identification of the authority for the disclosure under *FOIPOP* or the *MGA*.

If the disclosure is at the public body's initiative, the policy should require that the public body clearly identify its authority for disclosing the data without request to another organization.

6. Security

FOIPOP and the *MGA* both require that personal information be protected using reasonable security arrangements. The security section of the policy should describe, in general terms, the security arrangements for the video surveillance system and data. Such arrangements fall into four categories:

(a) Administrative security:
- Describe the process to follow if there is an unauthorized disclosure of images.

(b) Physical security:
- Set standards for locks, passcodes etc. for the servers and stored images. If monitors are used, ensure that monitors are installed in a secure area and viewable only by authorized employees. If images are available online, ensure that only authorized users can access the images and that such access is automatically logged by the system.

(c) Technical security:
- Describe in general terms the technical security required. For example, whether the data will be encrypted, and what the requirements are for regular security updates, patches, etc.
- If the system you have purchased uses wifi technology you must carefully evaluate the security of this function. Wireless transmissions like CCTV (closed-circuit television) broadcasts are inherently subject to interference and interception, especially when they use publicly available frequency bands. CCTV signals are generally not encrypted or secured and may easily be captured by others with an appropriately tuned receiver. As there are only a limited number of transmission channels, the chances of inadvertent interception are high.[2]

[2] As explained by the Office of the Information and Privacy Commissioner for Newfoundland in its guidance, *OIPC Guidelines for Video Surveillance by Public Bodies in Newfoundland and Labrador,* June 26, 2016 at p. 13.

(d) Personnel security:

- Designate the persons in the organization (described by position in the policy) who are authorized to operate the system and those who are authorized to view the data.
- Set out requirements for regular appropriate and ongoing training to operators to make certain they understand their obligations under privacy law and this video surveillance policy.

7. Retention

Video surveillance records create a number of risks for organizations. First, they are a collection of sensitive personal information that could be subject to a privacy breach. The more data you have, the more data that could be subject to unauthorized use or disclosure. Second, individuals have the right to request access to their personal information, including video surveillance. In order to disclose the information, public bodies and municipalities will have to purchase software that allows them to sever out images of other individuals if disclosure of those images would be an unreasonable invasion of personal privacy. This is an additional cost to organizations.

8. Access to Information and Correction Requests

Under *FOIPOP* and the *MGA* individuals are entitled to access copies of records containing their own personal information. Since "record" includes information "stored by graphic, electronic, mechanical or other means"[3] public bodies and municipalities must be prepared to provide copies of video surveillance data upon request. However, in order to do so, the public body may need to mask the images of third parties where the disclosure of these images would result in an unreasonable invasion of a third party's personal privacy. The policy should describe procedures for responding to access requests including how the public body or municipality will ensure that third party images are appropriately protected.

9. Contact information

Ensure that your policy includes contact information for your chief privacy officer or privacy lead. This person must be knowledgeable about the privacy implications of the video surveillance program.

[3] See s. 3(1)(k) of *FOIPOP* and s. 461(h) of the *MGA*.