Video Surveillance Guidelines

Office of the Information and Privacy Commissioner of Nova Scotia

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 the *Video Surveillance Policy Template* 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

Contents

Introduction

The purpose of this document is to assist public bodies and municipalities in Nova Scotia in deciding whether collection of personal information by means of video surveillance is both lawful and justifiable and if so, what privacy protection measures must be considered. The guidelines can be used to evaluate an existing video surveillance program or to determine whether and how to implement a new video surveillance program. Use the Video Surveillance Compliance Checklist at Appendix A to assess an existing video surveillance program against these guidelines and for ongoing review of new systems.

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 a statutory authority or authority of a search warrant to conduct the surveillance.

Video surveillance, or CCTV (closed-circuit television) as it is sometimes known, refers to any video surveillance technology (video cameras, still frame cameras, digital cameras and time-lapse cameras) that enables continuous or periodic recording (videotapes, photographs or digital images), viewing, or monitoring of public areas.

Video surveillance is common place in Nova Scotia. For example, in 2016 an informal survey of municipalities revealed that almost 70% of municipalities in Nova Scotia use some form of video surveillance.[1] None of the municipalities who reported employing video surveillance had conducted a privacy impact assessment of the surveillance before implementing it.

Public bodies and municipalities may have legitimate operational purposes for using CCTV systems, but cameras do not just capture particular incidents of crime, they also record the daily activities of anyone passing within view of the camera. Despite many international studies on the subject there is no clear consensus whether surveillance systems deter crime.[2]

FOIPOP & MGA: The Privacy Rules

The collection, use and disclosure of personal information by public bodies and municipalities in Nova Scotia is governed by rules set out in the *Freedom of Information and Protection of Privacy Act* (*FOIPOP*) and the *Municipal Government Act, Part XX* (*MGA*). The privacy rules in these two laws are virtually identical. Public bodies and municipalities cannot collect, use or disclose any personal information unless specifically authorized under these laws. Video surveillance collects personal information in the form of images of individuals participating in various activities from walking down a street to spray painting your front door with graffiti.

[1] The OIPC conducted a voluntary survey of 53 municipalities, districts, regions and towns in Nova Scotia in August 2016. Of the 53, 25 responded to the survey and 68% reported having video surveillance cameras. The average number of cameras reported was 8.25.

[2] The Office of the Information and Privacy Commissioner for Newfoundland and Labrador conducted a literature review prior to producing its video surveillance guidelines, *OIPC Guidelines for Video Surveillance by Public Bodies in Newfoundland and Labrador* in June 2015. This observation is based on that office's guideline at p. 2.

Step 1: Decide whether video surveillance is right for you

Before you decide to implement video surveillance, outline your proposal and then subject it to the following preliminary analysis by answering four questions:

1. Is the video surveillance demonstrably necessary to meet a specific need?
2. Is there a less privacy invasive way of achieving the same end?
3. Is the video surveillance likely to be effective in meeting that need?
4. Is the loss of privacy created by the surveillance proportional to the need?

1. Is the video surveillance demonstrably necessary to meet a specific need?

Begin by identifying the exact problem you want to solve. The need you identify must be pressing and substantial, of sufficient importance to warrant overriding the right of innocent individuals to be free from surveillance in a public place. Accordingly, concrete evidence of the problem to be addressed is necessary. This should include real evidence of the risks, dangers, crime rates, etc. Specific and verifiable reports of incidents of crime, public safety concerns or other compelling circumstances are needed, not just anecdotal evidence or speculation.

If you are evaluating an existing video surveillance program, identify the original purpose for the surveillance program. Then review the history of the use of the surveillance to see when, if ever, the surveillance has been used to address the identified problem. How many times since implementation has this occurred? Also look to see if the identified problem has ceased to occur and/or continues to occur but outside of the video surveillance area or despite the video surveillance.

Remember you are trying to establish if the surveillance is demonstrably necessary to meet a specific need. Once you have clear evidence of a need, consider how exactly the video surveillance is demonstrably necessary to meet the need. To evaluate the demonstrable need, list all of the other strategies you have tried to address the need. Identify why these strategies have not worked. Then describe exactly how video surveillance is necessary to address the specific need.

2. Is there a less privacy invasive way of achieving the same end?

Explain what less privacy invasive methods you have already tried to meet the identified need. Sometimes if the problem is vandalism for example, brighter lights, a change in the security guard's routine or better signage may be all that's necessary to reduce the problem. Sometimes even a change in façade can significantly reduce vandalism in the form of graffiti. For example, many cities have found that murals serve as a major deterrent to graffiti. Before implementing video surveillance you must document all of the less privacy invasive efforts that were attempted and the results of those strategies.

If you have an existing video surveillance system, consider testing a less privacy invasive alternative to video surveillance to see if it can achieve the same end.

3. Is the video surveillance likely to be effective in meeting that need?

If you have concluded that the surveillance is demonstrably necessary to meet a specific need, evaluate next whether video surveillance is likely to be effective in meeting that need. So, for example, if your identified need is to prevent crime in a certain area, how will video surveillance actually prevent crime? Certainly your implementation plan will have to call for live viewing of the surveillance, otherwise prevention cannot occur.

If you are evaluating an existing video surveillance program then you should have clear evidence of whether or not the video surveillance has been effective in meeting the identified need. Check historical records for the use of the video surveillance and compare it against the original identified problem. If necessary, conduct an investigation into the current scope of the originally identified problem. Does it still exist? Has your investigation determined that video surveillance had any effect at all on the problem? What evidence do you have to support your findings? If you conclude that video surveillance has been effective in meeting the identified need, which cameras, exactly, were effective in addressing the problem?

4. Is the loss of privacy created by the surveillance proportional to the need?

Once you have concrete, objective evidence that video surveillance is likely effective in meeting the need you have identified then move on to examine whether or not the loss of privacy created by the surveillance is proportional to the need. For example, if windows are repeatedly broken at a local community center, placing video surveillance at all community centers would be out of proportion to the identified need. So too would placing cameras inside of the centre if the only identified problem is windows from the outside. Likewise, if the vandalism only happens at night, collection of video images during the day would not be proportional to the identified need.

Reassess your video surveillance plan to reduce the scope so that any surveillance is clearly focused only on the problem identified. Strategies that limit periods of day for surveillance are better than always-on surveillance. Limit the number of cameras and have them only in locations where there is clear evidence of a problem identified as the rationale for CCTV. Reducing the scope of the surveillance and keeping it sharply focused on the identified problem will help to make the surveillance proportional to the need.

Conclusion

If you are able to answer "yes" to all four of the above-noted questions, then proceed with step 2. If you cannot answer yes to all four questions then video surveillance is not the solution to the problem. Cameras already in existence that do not satisfy this four-part test should be turned off.

Step 2: Have a clear plan that complies with privacy laws

1. Develop a business plan

Develop a business plan for the CCTV system setting out:

- The purpose of the system.
- The outcome(s) that you expect.
- The type of technology and equipment that will be used.
- How the system will be operated.

If you already have a video surveillance system in place, conduct an audit of the system including all of the elements above plus a description of the system as it is currently used – number of cameras, hours of operation, scope of view, access to records, list of staff (by position) who currently have access to the recordings, types of disclosures currently permitted, types of uses currently permitted and retention periods.

Ensure that there is a named individual responsible for the operation of the video surveillance system.

2. Conduct a privacy impact assessment

Using the privacy impact assessment (PIA) templates available on the OIPC website, conduct a complete privacy impact assessment of the proposed or current video surveillance business plan: https://foipop.ns.ca/publicbodytools.

By conducting a PIA you will ensure that the project is in compliance with Nova Scotia's privacy laws. The PIA will also assist you in identifying privacy risks and mitigation strategies and will ensure that you have a plan in place to mitigate those risks.

Adjust your business plan to ensure that the project addresses any privacy impacts identified through the PIA process.

At least once every two years review your privacy impact assessment to ensure that any new or emerging privacy risks have been identified and mitigated.

3. Consult with stakeholders

Before implementing video surveillance, public bodies and municipalities should determine if consultations should occur with relevant stakeholders and representatives of those potentially impacted to ensure the need of video surveillance is debated and to determine if there will be public support for the practice.

For instance, if you have employees who will be filmed by the cameras, you should definitely discuss this with them. Explaining the purpose for the CCTV and getting your staff on-side will make the system more effective. Also, talking to others can give you excellent information – such as indicating whether CCTV might cause you problems that you had not thought about.

Depending on the size of your system and the reasons for installing it, it maybe also be useful to consult with:

- citizens,
- public interest groups,
- local community groups,

- other businesses,
- other agencies similar to your own that use CCTV,
- security specialists,
- the police,
- the Information and Privacy Commissioner.

Adjust your business plan to ensure that the project addresses any privacy impacts identified through the consultation process.

4. Develop a video surveillance policy

Your video surveillance policy is the tool you will use to make clear to employees and citizens how and when video surveillance will be used. The policy should, among other things, explain the rationale and purpose of the surveillance; when and how monitoring and/or recording will be in effect; how recordings will be used; retention periods; procedures for secure disposal of the recordings; and a process to follow if there is an unauthorized disclosure. Use the video surveillance policy template available on the OIPC website to guide you in the development of your policy: https://foipop.ns.ca/publicbodytools.

5. Train staff on the use of the video surveillance system

Educating your employees on their roles and responsibilities, as defined in the policies and procedures you have developed, is an essential step to achieving an effective and compliant video surveillance program. How are employees to know what their individual duties and responsibilities are if they are not adequately trained on them? If employees are not aware of their roles and responsibilities, your institution may be at a greater risk of having a privacy breach. Accordingly, it is important that employees are trained to ensure that they understand the authorized and unauthorized uses of video surveillance and their duties and responsibilities under *FOIPOP* or the *MGA* with respect to your organization's video surveillance program.

Step 3: Implement best practices for design and installation of the video surveillance system

1. Limit the time your surveillance is active

Cameras that are live for certain times of the day or night are preferable to those that are turned on 24/7. Only monitor or record during the time period that meets your specific purpose. For instance, if you have experienced break-ins after hours, only use your cameras when the office is closed so you are not capturing images of employees and citizens.

2. Avoid unintended subjects

One of the unexpected consequences of video surveillance is that cameras can easily capture images of people who are not targets, which would not be authorized under *FOIPOP* or *MGA*.

- Position cameras to reduce unauthorized image capture. For example, a security camera should not capture images of passersby on the street.
- Avoid areas where people have a heightened expectation of privacy, such as change rooms, washrooms, or into windows.

3. Use adequate signage to notify the public

Post a clear, understandable notice about the use of cameras before citizens enter the premises and at the entrances to different areas within your property that are under surveillance (e.g.: parking lot). Notification is respectful of citizens' privacy rights and gives individuals the option not to enter. The sign should indicate plainly which area is under video surveillance and for what purpose, for example: "This property is monitored by video surveillance for theft prevention." It should also state the legal authority for collection of personal information via video surveillance and provide contact information for someone in your organization if individuals have questions about the surveillance.

4. Transmit and store any recorded images securely

Ensure that video surveillance images are securely transmitted. Surveillance equipment should be stored under lock and key to protect your employees, guests, customers, clients and your organization from the risks of a privacy breach. Don't remove images from your premises and always follow a strict storage protocol.

5. Destroy recorded images when they are no longer needed

Prepare a retention and destruction schedule to specify the length of time that surveillance records will be kept. We recommend a maximum of 30 days unless the record is used to make a decision that directly affects an individual – then the record must be kept for one year.[3] Decide when and how records will be destroyed. Safely and securely destroy recorded images when they are no longer required for business purposes. Document the destruction in your logs.

6. Limit access to recorded images to authorized individuals

Your video surveillance policy should identify who is authorized to access the recordings. You should only review the recorded images to investigate a significant security or safety incident, such as when you have reported a crime to the police. Make sure that the right training is provided to your operators on an ongoing basis, so that they know their obligations under all relevant legislation. Minimize the number of individuals who have access to the system, monitoring, or recordings. All access to video records should be logged.

---

[3] In accordance with s. 24(4) of *FOIPOP* and s. 483(4) of *MGA*.

Any disclosure of video surveillance recordings outside your organization should be authorized by the applicable privacy law and documented.

7. Open access to your video surveillance policy
Consider making your written surveillance policy available to the public. Citizens will appreciate your transparency and gain a better understanding of the purposes of the surveillance.

8. Consider right of access
Anyone whose image is captured by your surveillance video has the right to access their own personal images, so you must be prepared to provide a copy of the relevant surveillance recording upon request. When disclosing recordings, use masking technology to ensure that identifying information about other individuals on the recording is not revealed contrary to *FOIPOP* or the *MGA*.

Step 4: Review and evaluate the use of video surveillance

Periodically re-evaluate your need for video surveillance. Organizational needs change. An area that was once prone to high rates of criminal activity may, through development or other external factors, transform into a low crime area. Further, new, less intrusive means of achieving the same goals may become available. Accordingly, it is important that the necessity of your organization's video surveillance program regularly be considered to determine whether it is still justified in accordance with the requirements of *FOIPOP* or the *MGA*.

Conduct regular privacy training to ensure that all staff are aware of the policies and procedures with respect to the use of video surveillance.

Collect statistics about your CCTV system to allow you to assess its strengths and weaknesses. After a year of operation and at regular intervals afterwards, evaluate the operation of the system. Consider the original problem it was intended to address. How many times did the CCTV system actually address the problem? In addition, conduct an audit of the roles, responsibilities and practices of your organization's video surveillance program regularly to ensure that they comply with your policies and procedures.

Additional resources

The Office of the Information and Privacy Commissioner can provide comments on draft privacy impact assessments and video surveillance business plans. We can assist in identifying privacy risks and mitigation strategies. Our contact information is available on our website at: www.foipop.ns.ca.

Appendix A: Video Surveillance Compliance Checklist

The following checklist will help to ensure that an existing video surveillance program is in compliance with best practices as described in this guideline.

Guideline	Actions and practices	Date checked	By
Step 2.1	**Responsibility:** There is a named individual who is responsible for the operation of the system.		
Step 2.2	**PIA:** There is a completed privacy impact assessment. All mitigation steps have been completed.		
Step 2.2	**PIA Review:** The PIA has been reviewed in the last two years to ensure that any new or emerging risks have been identified and mitigated.		
Step 2.4	**Policy:** The video surveillance policy is complete, approved and up to date.		
Step 2.5	**Training:** All staff, including new staff, have received training on the proper use of the video surveillance system and have been provided with the video surveillance policy.		
Step 3.1	**Limit time of day:** Cameras are only operating during times they are needed to address identified problems.		
Step 3.2	**Unintended subjects:** Cameras are focused specifically on problem areas. Cameras do not capture unintended or unauthorized images.		
Step 3.3	**Adequate signage:** There are video surveillance notification signs near every video camera. All signs include an explanation for the purpose of the surveillance, legal authority for collection and contact information.		
Step 3.4	**Security:** Video surveillance images are transmitted and stored securely.		
Step 3.5	**Limited retention:** Video images are only retained for the approved retention periods.		
Step 3.6	**Limited access:** Only approved individuals have access to video surveillance images. Access logs are regularly checked to ensure all accesses to images are authorized.		
Step 4	**Regular review:** The system is regularly reviewed to ensure it is working properly.		

Notice to Users

This document is intended to provide general information only. It is not intended, nor can it be relied upon, as legal advice. As an independent agency mandated to oversee compliance with *FOIPOP*, *MGA* and *PHIA*, the Office of the Information and Privacy Commissioner cannot approve in advance any proposal from a public body, municipality or health custodian. We must maintain our ability to investigate complaints and to provide recommendations in response to these complaints. The contents of this document do not fetter or bind this office with respect to any matter, including any complaint investigation or other matter, respecting which the Commissioner will keep an open mind. It remains the responsibility of each public body, municipality and health custodian, to ensure that they comply with their responsibilities under the relevant legislation. Further information about our role and mandate can be found at: http://foipop.ns.ca.