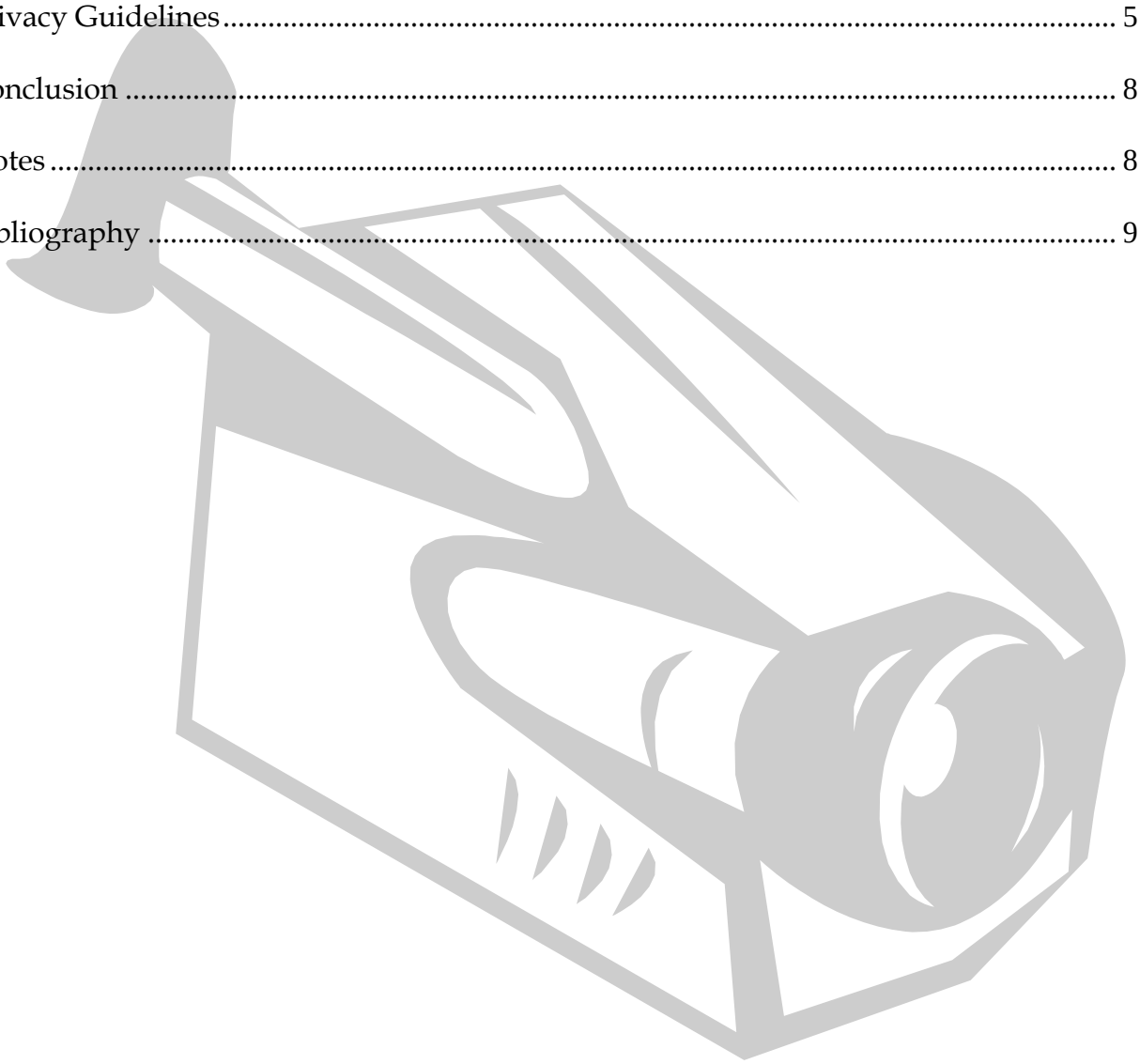
Office of the Information and Privacy Commissioner
for Newfoundland and Labrador

Guidelines for Video Surveillance by Public Bodies in Newfoundland and Labrador

May 2005

Table of Contents



The intent of this document is to assist public bodies in deciding whether collection of personal information by means of a video surveillance program/practice is both lawful and justifiable and, if so, what privacy protection measures must be considered.

Introduction

Video surveillance systems refer to any video surveillance technology (video cameras; closed circuit television 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. The technology that enables this video surveillance is readily available. A simple glance through the phone book will reveal a number of companies in this province which provide and service this type of equipment. One nationwide company advertises on its website that their surveillance equipment is "easily customized to meet your situation" including night-vision cameras, time-lapse recorders, wireless pinhole cameras, surveillance vans and covert body-worn video equipment.[1] The applications listed on this website include the prevention of property vandalism, employee theft, and spousal infidelity to name a few.

The idea of catching those guilty in the act may be enough for some individuals, companies, or public bodies to justify the use of video surveillance. Others may see video surveillance as a necessary and effective tool in deterring crime and protecting public safety. And some will insist that they actually feel safer knowing when they are in a public area that it is monitored by video surveillance. But, do the ends always justify the means? Public bodies may have legitimate operational purposes for using video surveillance 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. Does the use of surveillance systems deter crime? This has yet to be conclusively determined. A report in August 2003 suggests that, "*CCTVs are effective at reducing incidents of burglary and property crime, but they are not effective against personal crime, violent crime or public disorder*."[2]

The installation of surveillance cameras in public buildings (elevators, parking lots, entrances), and public areas (buses, parks, streets) is increasing in jurisdictions all over the world. Britain has over 1.5 million cameras covering public spaces across the country and these numbers continue to grow.[3] The situation is no different in New Zealand. A June 16, 2004 article reads, "*Surveillance cameras are now as much a part of everyday New Zealand life as computers and cellphones*."[4] As for Canada, the RCMP Commissioner Guilliano Zaccardelli is calling for national standards for the use of surveillance cameras and quoted, "*I don't want Canada to become a country where there is a camera on every street corner or on every building*."[5] How commonplace is video surveillance in Newfoundland and Labrador? To our knowledge no comprehensive survey has taken place to determine the extent of the use of video surveillance by public

bodies, but some evidence exists to show that it is becoming more and more commonplace. A CBC television piece which aired in early 2005 reported on the installation of video cameras at a high school for the purpose of deterring unauthorized persons from entering the school, which had been a source of theft and vandalism. When we began to look at the practices of school boards across the province, we found that in quite a number of cases video cameras had been installed in schools and school buses.

Another television news piece which aired in early 2005 indicated that some nursing homes in the province were also beginning to use video cameras. The homes had experienced a number of security issues which they are now attempting to address through the use of video surveillance. A trip to Confederation Building will also reveal the use of video surveillance for security purposes, the most noticeable being cameras mounted high atop the rear of the building which monitor the parking area. A corresponding sign notifying visitors that video surveillance is in use is posted nearby.

Obviously, some public bodies have identified needs for using video surveillance. But, how do public bodies know what can be done legally with this "captured" information?

Legal Privacy Considerations

If images or voices of people are "captured" by video or audio recordings, privacy considerations come into play. The Office of the Information and Privacy Commissioner (OIPC) provides oversight to the law relating to the protection of personal information in Newfoundland and Labrador. Part IV of the *Access to Information and Protection of Privacy Act (ATIPPA)* sets out the law in relation to the collection, use, and disclosure of personal information in the possession or control of public bodies (government departments, agencies, Crown Corporations, municipalities, health care boards, Memorial University, schools, the College of the North Atlantic, etc.). The *ATIPPA* was proclaimed into law on January 17, 2005, but the privacy provisions (Part IV) are not expected to be proclaimed into law until early 2006 in order to give public bodies a further opportunity to ensure that they are in compliance.

All public bodies will be required to comply with the privacy protection provisions that govern the collection, use, and disclosure of personal information when Part IV of the *ATIPPA* is proclaimed into law. "Personal information" means "recorded information about an identifiable individual" and includes details such as your name, address, phone number, SIN or MCP number, driver's license number, and opinions of another person about you (s. 2 (o) *ATIPPA*). A record is information in any form and includes everything from documents, maps, books, handwritten notes, phone messages, photographs, and video recordings. Any record of the image or voice of an identifiable

individual is a record of personal information. This record and the public body's practices are subject to the privacy provisions of the *ATIPPA* once they come into force.

Collection of personal information under the *ATIPPA* must relate directly to and be necessary for the operation of a program or activity run by a public body, or be expressly authorized by another act, or be for the purpose of law enforcement. This indicates that public bodies must be able to demonstrate that any proposed or existing collection of personal information by video surveillance is for a specific purpose, necessary and lawful.

Some collections are obviously inappropriate. Diane Boissinot, the interim chairperson of the Quebec Access to Information Commission in a June 10, 2004 article said, "*If the city wants to use video surveillance to crack down on people discarding cigarette butts, for example, video surveillance is not appropriate. The price is too high to have clean sidewalks*," she said.[6]

Public bodies need to inform the impacted public when collecting personal information through video surveillance. This should be accomplished through the use of signage which provides details such as how the information will be used and who will be allowed to view it. The decision to collect, use or disclose personal information is the responsibility of "the head" of a public body, such as a Minister or CEO. Public bodies must follow rules as set out in the *ATIPPA* in relation to the use or disclosure of personal information.

Individuals have a right of access to their own records, regardless of what format they are in. In the case of surveillance recordings, the individual may request amendment or even destruction of the recording. Public bodies have a duty to protect the integrity of and the confidentiality of personal information through the establishment of policies and procedures to maintain administrative, technical, and physical safeguards. Video surveillance practices/programs must be the least intrusive possible, lawful, and justifiable. Each public body should complete a Privacy Impact Assessment (PIA) to assess the actual or potential effect of proposed video surveillance systems. A sample outline for a PIA can be made available by contacting the OIPC.

The next section looks specifically at recommended general privacy guidelines for consideration when a public body contemplates a video surveillance program or practice.

Privacy Guidelines

These guidelines do not constitute a decision or finding respecting any past or present investigation of the Information and Privacy Commissioner. The guidelines do not apply to covert (hidden) or overt (open) surveillance systems used by a public body as a case-specific investigation tool for law enforcement purposes, where there is statutory authority and/or the authority of a search warrant to conduct the surveillance.

These guidelines apply to video surveillance of public areas of facilities operated by public bodies. They are not meant to provide a framework for monitoring employee work performance through the use of video surveillance. Other considerations not discussed may be appropriate and required. These guidelines are only effective if applied collectively to a video surveillance program/practice.

1. Using video surveillance systems to address concrete, confirmed problems and/or incidents is acceptable only if the practice meets all statutory requirements and is utilized as a last resort outweighing the negative effect on personal privacy. Specific and verifiable reports of incidents of crime, public safety concerns, or other compelling circumstances are required to proceed. This does not include anecdotal evidence or speculation. The goals and/or purpose of the proposed program/practice must be clear and address these specific incidents/problems.

2. Prior to adopting a proposed video surveillance program/practice an assessment of the impact on privacy is recommended. A Privacy Impact Assessment (PIA) of the proposed video surveillance practice/program should occur to assess what effects the proposed program will have on privacy and identify ways to mitigate any adverse effects. A sample PIA form is available through the OIPC.

3. Public bodies should consider public consultations prior to introducing video surveillance and inform those impacted once adopted. Public consultation with relevant stakeholders and representatives of those potentially impacted will ensure the need is debated, and will determine if public support will be forthcoming. Prior to the beginning of a video surveillance program/practice, reasonable and adequate warning is necessary. Once the system is operational, clearly written public notification at the perimeter of each surveillance area is necessary to inform individuals that the area is or may be under surveillance. The notification should also include who is responsible for the surveillance, and contact information for who is available to answer questions about the surveillance program/practices.

4. The video surveillance must be lawful. Public bodies must determine if they have the authority to collect, use and disclose personal information under provincial

privacy laws, including the *ATIPPA* and the *Privacy Act*, before implementing video surveillance program/practices. The *Privacy Act* is another piece of legislation (which is not under the jurisdiction of the OIPC) which establishes a tort in civil law when someone violates another person's privacy. Public bodies should also consider the right of privacy guaranteed by the *Canadian Charter of Rights and Freedoms*.

5. The design and operation of video surveillance program/practice should minimize privacy intrusion to what is absolutely necessary to achieve its goals. Installation of recording equipment should be restricted to identified public areas and, if at all possible, be restricted to periods where there is a demonstrably higher likelihood of crime being committed and thus detected in that area. "Always-on" surveillance may not be appropriate. If staff are permanently assigned to monitor a video surveillance security system, it is recommended that they only make a recording when viewing a suspected infraction or a criminal act during monitoring. In some locations, the public and employees have a heightened expectation of privacy such as the washroom or change rooms. Equipment should not monitor these areas. Operators should be restricted in the ability to adjust or manipulate the equipment to capture images that are not appropriate.

6. System operators require privacy-sensitivity training. The public body should require employees and contractors to review and apply policies governing the use of the system's equipment and in performance of their duties and functions related to the system. This will include orientation and training addressing staff obligations under the relevant statutes on a regular basis. Employees and contractors should sign written agreements regarding their duties to protect confidentiality of personal information and understand the consequences of a breach of the public body's policy and the provisions of relevant statutes.

7. Safeguards must be in place to protect and secure the equipment and images displayed or recorded. Access to the system's controls and reception equipment and to the images it captures should be limited to authorized personnel only. This access will include individuals designated on a "need to know" basis only. Video monitors should be out of the view of the public. Policies should address when recorded images may be viewed, by whom they may be viewed, and outline record retention schedules. A log should be maintained documenting who has accessed and used the recordings. This should also note disclosures of recordings and list the authority under which they are being disclosed. All tapes and storage devices that are not in use should be stored securely in a locked area with limited access by authorized personnel only. Old storage devices must be securely disposed of. Disposal methods may include shredding, burning or magnetically erasing the personal information to prevent retrieval or reconstruction.

8. Individuals have a legal right to access their personal information collected by a video surveillance recording. Access to an individual's own personal information may be granted, in whole or in part, depending upon statutory exemptions applied under legislation and if exempt information can be reasonably severed (e.g. personal information of others). Policies and procedures must recognize this right and accommodate any access requests.

9. After making the decision to use video surveillance, the public body should adopt comprehensive policies and procedures to direct the program/practices. Policies and procedures should be in writing and clearly set out the following:

- the rationale and purpose of the system;
- provide system guidelines that include: the location and field of vision of equipment, list of authorized personnel to operate the system, when surveillance will be in effect, and whether and when recordings will be made;
- develop policies and procedures specific to providing notice (informing the public), providing access, use, disclosure, security, retention and destruction of records;
- each public body must have an *ATIPPA* Coordinator in place. Involve your *ATIPPA* Coordinator in a lead role so that they can be responsible for access requests and privacy compliance;
- outline responsibilities of all service providers (employees and contractors) to review and comply with policy and statute in performing their duties and functions related to the operation of the video surveillance system;
- schedule regular orientation, training, audit and evaluative components; and
- clarify consequences of breach of contract or policy. The review and updating of policies and procedures should occur as necessary.

10. Video surveillance programs/practices should be subject to annual audits. Contracts with outside consultants should contain audit clauses for the provision of surveillance services and systems. These audits should address any deficiencies immediately. Video surveillance programs/practices should be evaluated during this process to address whether they continue to be appropriate, effective, and necessary to attain the original goals. Results of audits should be publicly available to ensure transparency and openness. An audit should consider such aspects as:

- Do the initial grounds for installing a camera or cameras still exist?
- Have the expected results been achieved? If not, is video surveillance still warranted?
- The appropriateness of the type of cameras and the number of cameras;
- Has a more appropriate alternative been developed/suggested?
- Review the number of hours of recording per day and recording periods during the week/year.

Conclusion

Public bodies using video surveillance systems are required to comply with the *ATIPPA* and other relevant statutes. Prior to implementing a video surveillance system, or any new program with privacy implications, public bodies should seek legal advice and/or complete a PIA of the proposed program/system. Adoption of all of these guidelines is also encouraged by the OIPC.

For more information on video surveillance or other privacy considerations, contact the OIPC at 729-6309, or toll free at 1-877-729-6309.

The Office of the Information and Privacy Commissioner of Newfoundland and Labrador gratefully acknowledges the permission granted by the Saskatchewan Information and Privacy Commission to adapt material from their pamphlet "*Guidelines for Video Surveillance by Saskatchewan Public Bodies*." The sources listed below were cited in the Saskatchewan pamphlet.

Notes

[1] Back Track Investigations: www.backtrackcanada.com

[2] Greenhalgh, S (2003) Literature Review of Issues of Privacy and Surveillance Affecting Social Behaviour, p.1.

[3] Ward, K. Video surveillance debate heats up. The Canadian Press, October 6, 2002.

[4] Booker, J and Sue Allen, *Nowhere to hide: City surveillance*. Stuff.co.nz (New Zealand), June 16, 2004.

[5] Rusnell, C. CanWest News Service, Edmonton Journal, June 12, 2004.

[6] Dougherty, K. *Quebec Privacy Czar warns Montreal about CCTV use*. The Montreal Gazette (Quebec), June 10, 2004

Bibliography

Guide to Using Surveillance Cameras in Public Areas. Freedom of Information and Protection of Privacy, Government of Alberta, April 2001.

Privacy Guidelines for Use of Video Surveillance Technology by Public Bodies. Freedom of Information and Protection of Privacy, Ministry of Management Services, Government of British Columbia, April 22, 2002.

Investigation Report P98-012, Video Surveillance by Public Bodies: a Discussion. Information and Privacy Commissioner of British Columbia, March 31, 1998.

Greenhalgh, Stephen. *Literature Review on Issues of Privacy and Surveillance Affecting Social Behaviour*. Office of the Information and Privacy Commissioner of Alberta, August 2003.

Public Surveillance System Privacy Guidelines, OIPC Reference Document 00-01. Office of the Information and Privacy Commissioner of British Columbia, January 26, 2001.

Privacy and Human Rights 2003: Threats to Privacy. Available Online: www.privacyinternational.org/survey/phr2003/threats.htm.

Guidelines for Using Video Surveillance Cameras in Public Places. Information and Privacy Commissioner/Ontario, October 2001.