

GUIDELINES FOR VIDEO SURVEILLANCE BY SASKATCHEWAN PUBLIC BODIES

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 camera; 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. In Saskatchewan a company advertises on its website that their surveillance equipment is “easily customized to meet your situation” including night-vision cameras, time-lapse recorders, 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, but also the daily activities of anyone passing within view of the camera.

Does the use of surveillance systems deter crime? In Saskatchewan, as in the rest of Canada, this has yet to be 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 (in elevators, parking lots, entrances), and to monitor public areas (buses, in parks, on 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 Guillianio Zaccardelli is calling for national standards

¹ Saskatoon Back Track Investigations: www.backtrackcanada.com/surv.php

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

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 Saskatchewan? 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 peak our suspicions that the use of video surveillance may be widespread. As early as 1997, a newspaper article contemplated the practice. It reads, “*Regina city council has approved a plan to use closed-circuit television to fight crime and help the public feel safer.*”⁶ And, a quick search of the Saskatoon Public Library site’s Gallery page reveals the note: “*Please Note: Gallery premises are protected by video surveillance.*”⁷ Further, the College of Commerce in Saskatoon use agreement opens with, “*Use of the computer facilities is monitored by Video Surveillance and other means.*”⁸

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 three provincial laws that address the protection of personal information in Saskatchewan. Part IV of *The Freedom of Information and Protection of Privacy (FOIP) Act* and the *Local Authority Freedom of Information and Protection of Privacy (LA FOIP) Act* outline a complete code for the collection, use, and disclosure of personal information in the possession or control of government institutions (departments, agencies, Crown Corporations) and local authorities (municipalities, Regional Health Authorities, universities, schools, regional colleges, and library boards). The third provincial law, *the Health Information Protection (HIPA) Act*, sets out the rights of individuals and the obligations of “trustees” in the health system with respect to personal health information. Trustees are individuals and corporations who are part of Saskatchewan’s health system. The OIPC does not oversee *The Privacy Act (SK)*. This law makes the unreasonable invasion of privacy a civil tort with recourse to the Court of Queen’s Bench.

"Personal information" is "recorded information about an identifiable individual" and includes details such as your name, address, phone number, SIN, race, driver’s license number, health card number, credit ratings, and opinions of another person about you (s.

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

⁶ O’Connor, Kevin. Canadian Press NewsWire. Toronto: July 24, 1997

⁷ Saskatoon Public Library: www.publib.saskatoon.sk.ca/morrison_ga.html

⁸ College of Commerce – Technology Support Centre:
www.commerce.usask.ca/departments/techcentre/policy.asp

24 FOIP and s. 23 LA FOIP). Personal **health** information includes information about your physical or mental health and/or information gathered in the course of providing health services for you [s. 2(m) HIPA].

A record is information in any form or format and includes everything from documents, maps, books, handwritten notes, phone messages, photographs, to even, 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 FOIP Act, the LA FOIP Act, and HIPA. All public bodies designated by legislation are required to comply with the privacy protection provisions that govern the collection, use, and disclosure of personal information (PART IV).

Collection of personal information under the FOIP Acts (s. 26 FOIP and s. 25 LA FOIP) must be for the general purposes of a program, activity, or service or for a consistent use. Trustees must collect, use, or disclose only the personal health information that is reasonably necessary for a consistent purpose under HIPA (sections 23 and 24). These sections of the statutes indicate that public bodies must be able to demonstrate that any proposed or existing collection of personal information by a video surveillance programs/practices 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.⁹

Public bodies need to inform the impacted public when collecting personal information through video surveillance. This should include providing details on the anticipated uses and potential disclosures of that recorded information. Use is what the public body does with the information internally. Disclosure means to give out, release or make available to others outside of the organization.

Consent expectations (s. 18 FOIP Regs; s. 11 LA FOIP Regs; s. 5 of HIPA) are consistent throughout the different privacy laws in so much as each individual has a right to consent to the use or disclosure of his/her personal information (including personal health information) unless a provision of a statute authorizes otherwise. An example of when consent is not required is a disclosure to a prescribed law enforcement agency carrying out a lawful investigation.

The decision to disclose personal information is the responsibility of "the head" of a public body, such as a Minister, CEO, or an Administrator. For a disclosure to occur and not result in an unreasonable invasion of privacy, the head would have to effectively demonstrate which exception applies under the relevant statute.

⁹ Dougherty, K. *Quebec Privacy Czar warns Montreal about CCTV use.* The Montreal Gazette (Quebec), June 10, 2004

Under the provincial privacy laws, recorded individuals have a right of access to those recordings (s. 31 FOIP; s. 30 LA FOIP; s. 12 HIPA). In the case of surveillance recordings, the individual may request amendment or even its destruction.

HIPA clearly outlines the 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 (section 16). The same consideration should apply to all personal information collected through video surveillance by any public body, under the FOIP or LA FOIP Acts.

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 copy of the PIA is available at the OIPC website at www.oipc.sk.ca.

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 Saskatchewan 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 are not intended for the surveillance of those employed by a public body. 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 diminution of 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 necessary.

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. The PIA form is available on the OIPC website: www.oipc.sk.ca.

3. Public bodies should consider public consultations prior to introducing video surveillance and inform those impacted once adopted.

Public consultations of 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 surveillance areas 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 (FOIP, LA FOIP and HIPA) before implementing video surveillance program/practices. They 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.

Instillation of recording equipment should be restricted to identified public areas and be restricted to periods where there is a demonstrably higher likelihood of crime being committed and thus detected in that area. "Always-on" surveillance is not appropriate.

If video surveillance is necessary, consider limiting the operational times to times when there is a higher likelihood of a threat to safety of people and

property. If possible, 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 limited 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. The safeguarding of the equipment and images must occur.

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 to view recorded images, by whom, and outline record retention schedules.

A log should be maintained documenting access to and the uses of recordings. This will include disclosures of recordings and under what authority.

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 right to access their personal information.

Individuals have a legal right to access his/her 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 includes: 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;
- Specify a designated FOIP Coordinator 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 audit and evaluation.

Contracts should contain audit clauses for the provision of surveillance services and systems. These audits should occur periodically and address any deficiencies immediately.

Video surveillance programs/practices should be evaluated to address its appropriateness and effectiveness in attaining its original goals.

Results of audits and evaluations should be publicly available to ensure transparency and openness.

Conclusion

Public bodies using video surveillance systems are required to comply with statutory provisions. 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 (306) 787-8350.

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.