OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

OIPC Guidelines for Video Surveillance by Public Bodies in Newfoundland and Labrador

June 26, 2015

TABLE OF CONTENTS

Page

The intent of this document remains to assist public bodies in deciding whether collection of personal information by means of CCTV is both lawful and justifiable and, if so, what privacy protection measures (including policies and procedures) must be considered. Review of multiple academic studies over the past decade or more on CCTV and comprehensive analysis of both provincial and international guidelines have helped formulate this document.

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

The OIPC published separate guidelines for the use of CCTV in schools in February 2013. These guidelines can be found at the OIPC website as OIPC Guidelines for the use of Video Surveillance in Schools. **(http://www.oipc.nl.ca/pdfs/SchoolGuidelinesVideoSurveillance.pdf)**

Introduction

For the purposes of these guidelines CCTV 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. CCTV has been in common usage for approximately the past two decades, but its first known usage was over 70 years ago. It has become quite common throughout the world to see CCTV in stores, airports and banks, and it is becoming increasingly more likely for CCTV to be found in government buildings, on streets and even in schools. The technology that enables this video surveillance is readily available. Equipment including night-vision cameras, time-lapse recorders, wireless pinhole cameras, surveillance vans, broadcast capable camera systems, radio frequency identification systems, facial recognition software, automatic license plate recognition software, unmanned aerial vehicles (drones) and covert body-worn video equipment are all becoming common surveillance tools. So while the term CCTV is a bit antiquated in that it doesn't just cover overt surveillance cameras anymore, the term is still used in common vernacular to encompass a broad array of technology.

The idea of catching criminals or wrong-doers 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 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. In fact, conflicting studies point to displacement rather than deterrence; to prevention of crime in certain locations such as parking areas but not in other locations such as open streets; to prevention of certain crimes such as theft but not of others such as assault; and some studies show that while CCTV does not effectively deter crime, it does aid in the criminal investigation and prosecution fields.

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. The UK has over 6 million cameras covering public spaces across the country and these numbers continue to grow. New Zealand and Australia as well as most of Asia are now reporting vast increases in the use of CCTV.

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 evidence exists to show that it is becoming more and more commonplace. Over 25% of all K to 12 schools in Newfoundland and Labrador currently have CCTV in place, with all new schools being pre-wired for installation. The Multi-Materials Stewardship Board provides funding for municipalities to place CCTV systems near suspected illegal dump sites, and many towns/cities currently have CCTV in operation. The RNC have been running a CCTV operation on George Street in St. John's for a number of years. Locations including Confederation Building, airports, and nursing homes are also using CCTV technology.

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? Privacy is a

recognized fundamental right and must be balanced carefully with the use of any technology that captures personal information.

ATIPPA, 2015

The *Access to Information and Protection of Privacy Act* was passed by the Newfoundland and Labrador House of Assembly in March of 2002. The access provisions were proclaimed into force on January 17, 2005 and the privacy provisions were proclaimed into force on January 16, 2008. The *ATIPPA* was amended in 2012 and it was repealed in 2015, replaced by the current statute known as *ATIPPA, 2015*. The *ATIPPA, 2015* governs access to records in the custody of or under the control of a public body and sets out requirements for the collection, use, and disclosure of personal information contained in the records they maintain.

A public body is defined in section 2 of the legislation and includes provincial departments and agencies, school districts, public post-secondary institutions, health boards and municipalities.

The protection of privacy provisions (Part III) of the *ATIPPA, 2015* limit the extent and means by which public bodies can collect personal information, as well as the extent to which public bodies can use and disclose that information. Part III also requires public bodies to make every reasonable effort to ensure that personal information is accurate and complete, to make reasonable security arrangements against unauthorized access, collection, use, disclosure or disposal of personal information, and to retain certain personal information about an individual in order to allow that individual a reasonable opportunity to obtain access to the information.

It is important to recognize that an individual has the right to file a complaint with the Information and Privacy Commissioner if that individual has reasonable grounds to believe that his or her personal information has been collected, used or disclosed by a public body in contravention of the provisions of Part III of the *ATIPPA, 2015*. The public body under *ATIPPA, 2015*, would be the party required to respond to such a complaint. The Commissioner (or delegate) may investigate such a complaint, and if the complaint cannot be resolved informally, the Commissioner may make a finding as to whether or not the alleged collection, use or disclosure was in compliance with Part III of the *ATIPPA, 2015*. Whether or not the Commissioner finds that the public body has complied

with Part III, the Commissioner may report the findings of his investigation in a published report and/or in the Commissioner's Annual Report to the House of Assembly. If the Commissioner finds that the public body has acted contrary to the provisions of Part III, the Commissioner may also issue recommendations to ensure compliance with the *ATIPPA, 2015*. Also, if the Commissioner's recommendation is to stop collecting, using or disclosing personal information in contravention of *ATIPPA, 2015* and the public body fails to comply, he may prepare and file an order with the Trial Division.

Section 61 of the *ATIPPA, 2015* states:

> *61. No personal information may be collected by or for a public body unless*
>
> *(a) the collection of that information is expressly authorized by or under an Act;*
>
> *(b) that information is collected for the purposes of law enforcement; or*
>
> *(c) that information relates directly to and is necessary for an operating program or activity of the public body.*

Definitions

The following definitions are provided for assistance in interpreting these *Guidelines*:

- *Personal Information* as defined in the *ATIPPA, 2015* means recorded information about an identifiable individual, including

  (i) the individual's name, address or telephone number,

  (ii) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,

  (iii) the individual's age, sex, sexual orientation, marital status or family status,

  (iv) an identifying number, symbol or other particular assigned to the individual,

  (v) the individual's fingerprints, blood type or inheritable characteristics,

  (vi) information about the individual's health care status or history, including a physical or mental disability,

(vii) information about the individual's educational, financial, criminal or employment status or history,

(viii) the opinions of a person about the individual, and

(ix) the individual's personal views or opinions, except where they are about someone else;

This definition provides a non-exhaustive list of examples of what constitutes personal information. **The requirement that personal information must be "recorded information about an identifiable individual" is critical. A recorded CCTV image of an identifiable individual meets this definition**. Also, it is important to note that while these guidelines refer to public areas, CCTV in a staff only area may also constitute a collection of personal information, and as such should also comply with these guidelines.

- *Policy* refers to statements of the public expectations defining the boundaries for administrative and staff action in carrying out its role and mandate. Policies should reflect what is expected and be directed towards outcomes. Policies must be consistent with law.
- *Procedures* are usually associated with each policy, detailing how something is done and the administrative action necessary to implement the policy.
- *Record*, as defined in Section 2 of the *ATIPPA*, means a record of information in any form, and includes information that is written, photographed, recorded or stored in any manner, but does not include a computer program or a mechanism that produced records on any storage medium.
- *Storage Device* refers to a videotape, computer disk or drive, CD-ROM, computer chip, or other device used to store the recorded data or visual, audio or other images captured by a video surveillance system.
- *CCTV* refers to any video surveillance systems or any video surveillance technology (including but not limited to 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.

Collection of Personal Information Using CCTV Surveillance

Recording a person's image is a collection of personal information as defined by the *ATIPPA, 2015*. Prior to undertaking the installation of a CCTV surveillance system, public bodies should consider the privacy implications of such action. Public bodies should conduct due diligence and training with respect to privacy awareness among staff and undertake a **Privacy Impact Assessment** prior to implementation.

Public bodies should draft policies and procedures that outline the roles and responsibilities of individuals or groups involved in the collection of personal information by CCTV.

Without limiting the content of these policies and procedures they should include:

- privacy-specific criteria that must be met before CCTV surveillance is undertaken including a description of alternative measures undertaken and their result;
- documentation of the decision, including a detailed rationale and purpose for the surveillance;
- written authorization at an appropriate level of the organization for undertaking video surveillance;
- limits on the collection of personal information to that which is necessary to achieve the stated purpose, including a description of the kind of information collected through the surveillance;
- limits on the use of the surveillance to its stated purpose and the duration of surveillance;
- details on the times when surveillance will be in effect and whether and when recording will occur;
- 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;
- limits on any special capabilities of the system, for example, sound, zoom, facial recognition or night-vision features;
- requirements that any recorded surveillance data or images be stored in a secure manner, including guidelines for managing video surveillance recordings, such as security, use, disclosure,

and retention and appropriate details on the place where signals from the equipment will be received and monitored;

- designations of the persons in the organization authorized to operate the system, including the names of the individuals who may have viewed the surveillance and what the surveillance was used for;
- procedures for the masking of and/or removal of third party information;
- a retention period for the surveillance;
- procedures for disposal of images including details on when and how images are to be disposed of;
- a service agreement with any third party hired to conduct the surveillance, if applicable;
- requirements that appropriate and ongoing training is provided to operators to make certain that they understand their obligations under all relevant legislation including *ATIPPA, 2015*, these Guidelines, and the organization's video surveillance policy;
- details on the process to follow if there is an unauthorized disclosure of images;
- procedures for individuals to access their own personal information captured through CCTV in compliance with the access provisions of the *ATIPPA, 2015*;
- sanctions for the organization's employees and contractors for failing to adhere to the policy; and
- the name and business contact information of the individual accountable for privacy compliance who can answer any questions or address concerns about the surveillance.

How to Decide Whether to Use a Video Surveillance System?

Prior to installing CCTV or before deciding whether to expand or continue utilizing the CCTV systems already in place, the first and paramount consideration is as follows:

> ***Is there a real, pressing and substantial problem which is ongoing in nature that has not and cannot be mitigated by other less privacy intrusive measures?***

One incident, no matter how serious or severe, does not constitute a real, pressing and substantial problem. Nor does a series of minor incidents constitute a real, pressing and substantial problem. Public bodies must determine if there is a problem that requires the use of CCTV systems.

Specific, ongoing 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 purpose of the proposed CCTV system must be clear, and the use of CCTV must be necessary to address the specific incidents or problems which have been identified. This means that less privacy-invasive measures must be evaluated, and where practical, implemented, to see whether the issue can be addressed through such measures, prior to the installation or usage of a CCTV system. Less privacy-invasive measures should be utilized unless they are ineffective or not feasible.

The following are other essential considerations for making a decision to decide whether or not to use CCTV:

1. **Has the impact of the proposed CCTV system on privacy been assessed?**

   A Privacy Impact Assessment of the proposed CCTV system should be conducted by the public body to determine the actual or potential kind and degree of interference with privacy that will result, and the ways in which adverse effects will be mitigated.

2. **Has the public been consulted?**

   It is recommended that public consultation be conducted with relevant stakeholders, including representatives of communities that will be affected. Prior to the installation of CCTV systems, public bodies should notify individuals and groups of the intention to consider installation of CCTV. The specific rationale for a CCTV system should be explained, and there should be an opportunity to ask questions and debate other ways in which both privacy and security can be protected and maintained while addressing the issues which gave rise to the decision to explore the use of CCTV. Public bodies should also be able to explain the legal authority for the collection of personal information through CCTV. Notification should consist, at a minimum, of a memo/letter/newsletter to affected individuals, and posting of the information on the

public body website. Public meetings with affected individuals are also suggested. Any written notices or memos should outline the principal purpose(s) for which CCTV is intended to be used and the name, title and contact information of someone who can answer questions about it. Regardless of the outcome of the consultation, public bodies must still be able to support the use of CCTV on the basis, as noted above, that there is a real, pressing and substantial problem which is ongoing in nature that has not and cannot be mitigated by other less privacy intrusive measures.

3. **Is the CCTV system consistent with applicable laws including *ATIPPA, 2015*?**

CCTV systems must be consistent with all applicable laws, including overarching laws such as the *Canadian Charter of Rights and Freedoms* and the *ATIPPA, 2015*.

4. **Has the CCTV system been designed to minimize the impact on privacy?**

The surveillance system should be designed and operated so that the privacy intrusion it creates is no greater than absolutely necessary to achieve the system's goals. For example, limited use of video surveillance (e.g., for limited periods of day, peak periods when problems have typically occurred) should be preferred to always-on surveillance if it will achieve substantially the same result. Furthermore, cameras should be limited to only those locations which are necessary to address the problem(s) identified as the rationale for CCTV. Privacy enhancing technology such as encryption of files or available face blurring technology might be useful.

5. **Has the public been advised that they will be under surveillance?**

The public should be informed with clearly written signs at the perimeter of surveillance areas, which advise that the area is or may be under surveillance, and indicate who is responsible for the surveillance, including who is responsible for compliance with privacy laws, and who can be contacted to answer questions or provide information about the system.

6. **Does the public body have fair information practices in place for the collection, use, disclosure, retention and destruction of personal information?**

The information collected through video surveillance should be minimal; its use should be restricted, its disclosure controlled, its retention limited, and its destruction assured. If a camera is manually controlled or actively monitored, the recording function should only be turned on in the event of an observed or suspected infraction. If an unmonitored camera records continuously, the recordings should be conserved for a limited time only, according to a retention schedule, unless a serious incident has been captured or the recordings are relevant to a criminal act that has been reported to the police. Information collected through video surveillance should not be used for any purpose other than the purpose that law enforcement or another body with legal authority to do so has explicitly authorized. Any release or disclosure of recordings should be documented.

7. **Does the CCTV system eliminate or minimize excessive or unnecessary intrusions on privacy?**

Surveillance cameras should not be present in areas where people have a heightened expectation of privacy: for example, into windows of buildings, showers, washrooms, change rooms, etc. If cameras are adjustable by an operator, reasonable steps should be taken to ensure that they cannot be adjusted or manipulated to capture images in areas that are not intended to be under surveillance.

8. **Are the CCTV system operators sensitive to privacy issues?**

The operators of surveillance systems, including operators hired on contract, should be fully aware of the purposes of the system, and fully trained in rules protecting privacy. Operators and users of the CCTV system and recordings should sign confidentiality agreements.

9. **Are there assurances that the security of the equipment and images is protected?**

Access to the system's controls and reception equipment, and to the images it captures, should be limited to persons authorized in writing under the public body's policy. Recordings should be securely held, and access within the organization limited to a need-to-know basis.

10. **Are the rights of individuals to have access to their personal information respected?**

People whose images are recorded have a right under *ATIPPA, 2015* to request access to their recorded personal information, including their image recorded by CCTV. Severing the personal information in a recording (including software to implement blurring or blocking of the identities of others) may be necessary to allow individual access. Policies and procedures must accommodate such requests.

11. **Is the CCTV system subject to compliance review and evaluation?**

The system's operations should be subject to a regular compliance review and evaluation intended to identify any unintended negative impacts on privacy. In ideal circumstances a compliance review and evaluation should be conducted by persons or organizations independent of the management and direction of the video surveillance system. However, if financial challenges or other difficulties associated with contracting an external third party to do this work would prevent or unreasonably delay it, it is recommended that internal compliance reviews be conducted. Compliance reviews should ensure compliance with the *ATIPPA, 2015* as well as the policy governing the system, including ensuring that only pertinent information is collected, that the system is used only for its intended purpose, and that privacy protections in the system are respected. Evaluation should take special note of the reasons for undertaking surveillance in the first place, as determined in the initial statement of the problem and the public consultation, and determine whether video surveillance has in fact addressed the problems identified at those stages. Evaluation may indicate that a video surveillance system should be terminated or reduced in scope, either because the problem that justified it in the first place is no longer significant, or because the surveillance has proven ineffective in addressing the problem. Evaluation should take into account the views of different groups in the community (or different communities) affected by the surveillance. Results of compliance reviews and evaluations should be made publicly available.

12. **Does the public body have an explicit policy on the use of CCTV surveillance?**

As described above in the section entitled "Collection of Personal Information Using CCTV Surveillance," a comprehensive written policy governing the use of the surveillance equipment should be developed.

13. **Is there a mechanism in place to notify the public that the CCTV system has been adopted?**

Public bodies should recognize that individuals will want information about video surveillance systems. They may seek to know, for example, who has authorized the recording, whether and why their images have been recorded, what the images are used for, who has access to them, and how long they are retained. Public bodies should be prepared to provide this information.

Designing, Installing and Maintaining a Video Surveillance System

The CCTV surveillance system should be set up and operated to collect the minimum amount of information necessary to effectively achieve its intended purpose. This helps reduce the intrusion on individuals' privacy. Specifically, we make the following recommendations:

- Cameras that are turned on for limited periods in the day are preferable to "always on" surveillance.
- Cameras should be positioned to avoid capturing images of individuals in areas which are not being targeted. The field of view or angle of view should be large enough to capture the optimum view for the purpose of installation, however should be small enough to avoid unnecessary privacy intrusion.
- Cameras should not be present in areas where people have a heightened expectation of privacy, for example, showers, bathrooms, change areas, staff rooms or into windows. Steps should be taken to ensure that cameras cannot be adjusted or manipulated by the operator to capture images in such areas.
- Sound should not be recorded unless there is a specific and demonstrable need to do so. Sound recording represents an additional and even more significant layer of privacy

intrusion, and therefore a decision to consider recording sound must follow a rigorous analysis. Sound recording should not be viewed as a routine element of CCTV.

Wireless technology poses additional security and privacy risks and should not be employed unless all necessary precautions are taken. Wireless video surveillance systems, or wireless CCTV, typically refer to systems that transmit wireless signals to monitors. Commercially available systems do not normally have privacy or security designed into the transmission of the signal. As a result, such systems are easy to install but may allow unauthorized access unless special precautions are taken. Wireless transmissions like CCTV 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.

As a general rule, wired solutions are more secure than wireless solutions due to the reduced likelihood of interception. If a wired solution is not available, or if wireless is required for some other purpose, then the public body is responsible for ensuring that the security provisions of the system meet privacy requirements. The best way currently available to prevent the viewing of intercepted messages is by utilizing an encrypted, or scrambled, signal.

Notification and Signage After CCTV Installation

After installation public bodies should notify and inform individuals of the legal authority for the collection of personal information; the principal purpose(s) for which the personal information collected through CCTV is intended to be used and the name, title, and contact information of someone who can answer questions about that collection. Notification should consist, at a minimum, of signage and posting on the public body's website. Social media may be used as an additional means of notification.

Public bodies should use clearly written signs, prominently displayed at the perimeter of the video surveillance area, of CCTV equipment locations, so that each person has reasonable and adequate warning that surveillance is, or may be, in operation. At a minimum, there should be a sign in place

that notifies individuals of the recording and informs them that they may contact the public body with any questions.

Use of Video Surveillance Records

Information collected through CCTV surveillance should only be used for the purpose for which that surveillance has being undertaken. In other words, there must be a clear and specific rationale for installing CCTV, and personal information gathered through CCTV should only be used for purposes directly connected with that rationale. Public bodies should have clearly defined policies and procedures for the use of CCTV surveillance records. The public body is responsible for the content of the policies and procedures, including meeting the minimum standards as set out in these Guidelines.

Any information obtained through CCTV surveillance systems may only be used for purposes set out in the public body's policies and procedures and must relate to the protection of the public or property, or it must assist in the detection and deterrence of criminal activity and serious vandalism. Information should not be retained or used for purposes other than those described in the policy. For example, CCTV installed to prevent ongoing vandalism after normal working hours should not be used to deal with human resource matters during the work day.

Policies and procedures established by the public body should:

- Clearly state who can view/use the information and under what circumstances it may be viewed/used. The number of persons who may view the recorded information should be limited to specific individuals, such as the appointed CCTV director or ATIPP Coordinator and a designated alternate.
- Ensure that circumstances warranting a review of recorded CCTV images should be limited to instances where a serious incident has been reported/observed or to investigate a potential crime.
- Provide that where real-time viewing of the monitors takes place, the authority to view the monitors may only be delegated by the director to a limited number of individuals.

- Provide for logs of who accesses, uses or otherwise views information.
- Establish that electronic logs be kept if the technology to do so is available.
- Clearly state that CCTV surveillance should not be used for monitoring staff performance.

Disclosure of Video Surveillance Records

Personal information must not be disclosed except in accordance with *ATIPPA, 2015*. Because CCTV surveillance systems create a record by recording personal information, public bodies with a CCTV system should implement written policies and procedures and ensure that these are adopted.

Policies and procedures established by the public body should:

- Clearly state who is responsible for deciding to disclose images or other information from CCTV systems and under what circumstances these images or information may be disclosed.
- Provide for logs of who the information is disclosed to and for written confirmation of receipt of the information by the person who has received it.
- Clearly state that CCTV surveillance images can only be disclosed in compliance with the *ATIPPA, 2015*.

Retention of Video Surveillance Records

Public bodies should have clearly defined policies and procedures for the retention of CCTV surveillance records. The public body is responsible for the content of these policies and procedures, including meeting the minimum standards as set out in these Guidelines.

All recorded images must be stored in a secure location, and access should be granted only to a limited number of authorized individuals. All recordings that are not in use should be stored securely in a locked receptacle located in a controlled-access area or if stored electronically, with appropriate security to prevent unauthorized access. Each physical storage device that has been used should be dated and labeled with a unique, sequential number or other verifiable symbol.

Policies and procedures established by the public body should:

- Ensure that logs are kept of all instances of access to, and use of, recorded material, to provide for a proper audit trail.
- Set out the retention period for information that has not been viewed for the purpose of protecting public safety or to deter, detect, or assist in the investigation of criminal activity. Recorded information that has not been used in this fashion should be routinely erased according to a standard schedule. Unused recordings that are not viewed should be erased on a schedule not exceeding one month. The relevant retention periods should be clearly documented in both the public body policy and in the procedures;
- Establish a separate retention period when recorded information has been viewed for the purpose of protecting public safety or to deter, detect, or assist in the investigation of criminal activity. The length of this retention period may be established by the public body but should not exceed a reasonable period for which the personal information may be used for the aforementioned purpose.
- Require the public body to store and retain storage devices required for evidentiary purposes according to standard procedures until the law enforcement authorities request them. A storage device release form, or an entry in a logbook, should be completed before any storage device is disclosed to the appropriate authorities. The form should indicate who took the device, under what authority, when this occurred and if it will be returned or destroyed after use. This activity should be regularly monitored and strictly enforced.
- Establish that electronic logs should be kept where records are maintained electronically.

Disposal of Video Surveillance Records

Recordings should only be kept as long as necessary to fulfill the purpose of the CCTV surveillance. Recordings no longer required should be destroyed. Public bodies must ensure that the destruction is secure.

Policies and procedures established by the public body should:

- Establish who is responsible for ensuring the safe and proper disposal/destruction of storage devices.
- Ensure that old storage devices must be securely disposed of in such a way that the personal information cannot be reconstructed or retrieved. Disposal methods could include overwriting electronic records, shredding, burning or magnetically erasing the personal information.
- A storage device disposal/destruction form, or an entry in a logbook, should be completed before any storage device is disposed of and/or destroyed. The form should indicate who disposed of/destroyed the device, under what authority, when this occurred and what method of destruction/disposal was utilized.

Access to Personal Information

ATIPPA, 2015 establishes that individuals have the right to access their own personal information, including their own images as recorded by CCTV. When disclosing recordings to individuals who appear in them, the public body must ensure that identifying information about any other individuals on the recording is not revealed. This can be done through technologies that mask identity.

Policies and procedures established by the public body should:

- Clearly state who is responsible for deciding to provide access to the information and under what circumstances it was accessed.
- Provide for logs of who was given access to the information and when.
- Clearly state that CCTV surveillance is accessed for a specific purpose and is to be used only for that purpose.

Privacy Impact Assessment

A privacy impact assessment (PIA) is a formal evaluation of the privacy implications within a specific project. The term "project", in this context, is very broad; it refers to a project, program, initiative, legislation, system, application, program, or any other defined course of endeavor. Section 2 (w) of the *ATIPPA, 2015* defines a PIA as "… an assessment that is conducted by a public body … to determine if a current or proposed program or service meets or will meet the requirements of Part III of this Act…"

A PIA is a comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use or disclosure of personal information. It may also define the measures used to mitigate and, wherever possible, eliminate the identified risks.

The *ATIPPA, 2015* states:

> *72. (1) A minister shall, during the development of a program or service by a department or branch of the executive government of the province, submit to the minister responsible for this Act*
>
> *(a) a privacy impact assessment for that minister's review and comment; or*
>
> *(b) the results of a preliminary assessment showing that a privacy impact assessment of the program or service is not required.*
>
> *(2) A minister shall conduct a preliminary assessment and, where required, a privacy impact assessment in accordance with the directions of the minister responsible for this Act.*
>
> *(3) A minister shall notify the commissioner of a common or integrated program or service at an early stage of developing the program or service.*
>
> *(4) Where the minister responsible for this Act receives a privacy impact assessment respecting a common or integrated program or service for which disclosure of personal information may be permitted under paragraph 68 (1)(u), the minister shall, during the development of the program or service, submit the privacy impact assessment to the commissioner for the commissioner's review and comment.*

While section 72 requires a PIA from departments or branches of the executive government of the province, the OIPC strongly urges all public bodies and local public bodies that are contemplating the use of CCTV systems conduct a PIA prior to reaching a decision on the installation of a CCTV system. The PIA, while addressing *ATIPPA, 2015* should also focus on privacy in a wider context and the impact the CCTV system has on privacy. It should look at the pressing need the surveillance system is supposed to address, and show whether or not the system will meet this need. It should be based on reliable evidence and show whether the surveillance system proposed can be justified as proportionate to the needs identified. Where the system is already in use, the same issues should be considered and modifications should be made where a less privacy intrusive method could be used to address the pressing need.

While Section 72 of the *ATIPPA, 2015* requires departments or branches of the executive government to submit PIAs for common or integrated programs or services to the OIPC, any public body or local public body conducting a PIA is welcome to submit the PIA to the OIPC for review.

Without limiting the scope of the PIA for a CCTV system it is important to address the following issues: general rationale for the introduction of CCTV and background to the installation of the program; technical specifications of the cameras and their locations; ownership and management of the system; objectives of the system; accountability and complaints procedures; management of the control room; and retention of and access to recorded images.

Additional information on PIAs is available on the OIPC's website (PIA Guidance Document) and in the Government of Newfoundland and Labrador's Protection of Privacy Policy and Procedures Manual.

Reviewing and Evaluating the Use of Video Surveillance

Public bodies should ensure that the use and security of video surveillance equipment are subject to regular compliance reviews and evaluations. These compliance reviews and evaluations should also address the public body's compliance with operational policies and procedures. An external body

may be retained in order to perform the audit where possible. Any deficiencies or concerns identified by the audit must be addressed as soon as possible.

Employees and service providers should be aware that their activities are subject to such a review and that they may be called upon to justify their use of CCTV surveillance.

Public bodies should regularly review and evaluate the CCTV surveillance program in order to ascertain whether it is still justified in accordance with the requirements. This should include an assessment of whether the deployment of cameras at a particular location remains justified, or whether CCTV programs should be decreased or increased in scope. This evaluation should occur in a timely manner.

Tips for limiting the privacy impact of a CCTV system:

- Only install cameras in problem areas identified at the time the decision was made to proceed with CCTV. For example, if the justification for CCTV was vandalism to the exterior of a property, there may be no need for cameras inside the building.
- Activate cameras only during those times when the problems which led to the CCTV installation have occurred or are likely to occur in order to deal only with the identified problem. If there has been damage to the inside of a property due to break-ins on evenings or weekends, only turn on the cameras after the regular working hours of the operation. That way, the CCTV will capture the image of anyone who has broken in to vandalize or steal from the building, but will not impact the privacy of staff or visitors. If there have been criminal activities or serious vandalism inside the building, when do these activities normally occur? If these problems generally occur after regular working hours when parts of the building are not occupied, turn on the cameras for those periods of time only.
- The Office of the Information and Privacy Commissioner is available to consult with public bodies at any time. As the oversight body for *ATIPPA, 2015*, we are in a position to make recommendations to help ensure compliance with that law, and we are willing to work with all stakeholders to help ensure that privacy can be protected while meeting other operational and security needs.

Conclusion

In an October 2014 interview Jonathon Bamford of the UK's Information Commissioner's Office stated:

> "Surveillance cameras should not be deployed as a quick fix, but a proportionate response to a real and pressing problem. Putting in surveillance cameras or technology like automatic number plate recognition and body worn video is often seen as the first option, but before deploying it you need to understand the problem and whether that is an effective and proportionate solution. Failure to do proper privacy impact assessments in advance has been a common theme in our enforcement cases."

Public bodies using video surveillance systems are required to comply with the *ATIPPA, 2015* 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 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.