Privacy and School Bus Cameras

Renee Barrette, Director of Policy
Lauren Silver, Policy Analyst

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Canadian Pupil Transportation Conference

May 14, 2018

Objectives

- General understanding of Ontario's privacy laws and the role of the Information and Privacy Commissioner of Ontario (IPC)
- How the privacy laws apply to close-circuit television (CCTV) camera systems
- Steps your organization should take to ensure compliance with the law

Agenda

- Mandate and Role of the IPC
- *MFIPPA* Privacy Overview
- Privacy Complaints and Privacy Breaches
- Implementing School Bus Cameras
- Key Obligations under the *MFIPPA*
- Best Practices
- IPC Guidance Documents
- New Legislation Re: School Bus Cameras in Ontario
- Questions?

Our Office

- The mandate of the IPC is to provide an independent review of government decisions and practices concerning access and privacy, conduct research and education, and comment on proposed legislation and programs

- The Commissioner is appointed by and reports to the Legislative Assembly and remains independent of the government of the day to ensure impartiality

The Three Acts

The IPC oversees compliance with:

- *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)
- *Freedom of Information and Protection of Privacy Act* (*FIPPA*)
- *Personal Health Information Protection Act* (*PHIPA*)

New Mandates:

- *Child, Youth and Family Services Act, 2017* (Part X)
- *Anti-Racism Act, 2017*

Privacy in the Private Sector

- Ontario does not have its own private-sector privacy law
- The Privacy Commissioner of Canada oversees the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)
- *PIPEDA* applies to commercial businesses in Ontario (banks, airlines, retail stores etc.)

Fair Information Practices

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure, Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

Application of *MFIPPA*

- *MFIPPA* applies to "institutions" regarding the personal information in their custody and control

- Institutions under *MFIPPA* include school boards

- School boards remain responsible for the information practices associated with school bus programs – including programs that have been outsourced to a consortium

MFIPPA Privacy Overview

Privacy

- *MFIPPA* protects the privacy of individuals concerning their personal information while providing them with the right to access that information
- *MFIPPA* establishes rules for the collection, use, and disclosure of personal information
- For information in a record to qualify as personal information, it must be reasonable to expect that an individual may be identified if the information is disclosed

What is Personal Information?

- Recorded information about you
- Name, address, sex, age, education, and medical or employment history
- Any identifying number or symbol assigned to the individual (e.g., a licence plate)
- Video images of an individual (e.g., pedestrians and students)
- Personal views or opinions

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Fact Sheet

What is Personal Information?

October 2016

INTRODUCTION

The *Freedom of Information and Protection of Privacy Act (FIPPA)* and the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* (the acts) protect the privacy of personal information while providing individuals with a right of access to their own information.

In this fact sheet, we provide guidance about how the Information and Privacy Commissioner (IPC) interprets the term "personal information."

HOW IS PERSONAL INFORMATION DEFINED IN THE ACTS?

The acts define personal information as "recorded information about an identifiable individual," and include a list of examples of personal information (see Appendix A for the full definition).

Recorded information

Information can be recorded in any format, such as paper records, electronic records, digital photographs, videos or maps.

About an identifiable individual

Information is about an identifiable individual if:

- it is about the individual in a personal capacity; that is, it reveals something of a personal nature about the individual, and
- it is reasonable to expect that an individual can be identified from the information (either alone or by combining it with other information)

The listed examples include a person's name when combined with other information about them, such as their address, sex, age, education, or medical history. These examples are not exhaustive and many other kinds of information may still qualify as personal information.

What is not Personal Information

Personal information does **NOT** include:

- Information associated with an individual in a professional, official or business capacity, for example:
  - names of individuals who provided services to an institution on a fee-for-service basis
  - information relating to business costs incurred by named employees during the course of their employment as public employees

Privacy Obligations under the Act

MFIPPA sets out rules for the collection, use, and disclosure of personal information

To collect personal information, it must be:

- Expressly authorized by statute
- Used for the purposes of law enforcement, or
- Necessary to the proper administration of a lawfully authorized activity

Example:

Government institutions must have a legitimate reason and purpose for collecting personal information, such as a school board installing cameras to protect the safety and security of its students

You can only use personal information for:

- The purpose it was collected
- A consistent purpose or with consent (preferably in writing)

Example:

Video footage collected by a security camera cannot be used to monitor student attendance, but it may be used in relation to a security incident

You can only disclose personal information:

- With consent
- For a consistent purpose
- To comply with legislation
- For law enforcement
- For health and safety reasons
- For compassionate reasons

Example:

A video capturing evidence of a crime can be shared with law enforcement, even if it contains personal information

Notice

- In general, if an institution collects personal information, they must notify the individual to whom the information relates of the following:
  - the legal authority for the collection,
  - the principal purpose(s) for which the personal information is intended to be used, and
  - the title, business address and business telephone number of an officer or employee of the institution who can answer the individual's questions about the collection.

Privacy Breaches and Privacy Complaints

Privacy Breaches

- A privacy breach occurs when personal information is collected, retained, used or disclosed in ways that are not in accordance with the act
- Among the most common breaches of personal privacy is the unauthorized disclosure of personal information, such as:
  - Sending communications to the wrong recipient due to human error
  - Improper records destruction procedures
  - Loss or theft of unsecured assets, such as laptop computers, digital cameras, or portable storage devices (USB sticks)

Cont'd

Privacy Breaches

The IPC:

- May receive privacy complaints from the public or investigate on its own accord
- May investigate privacy complaints and report publicly on them
- Can order the institution to cease and destroy a collection of personal information
- May make recommendations to safeguard privacy

Privacy Complaints

IPC Privacy Complaint MC13-60

- Cameras aimed within the school's property were appropriate, but not the recording of images from outside the school's property
- IPC recommended that the school make changes to the video surveillance system to ensure that the cameras were not recording images outside the school's property

School Bus Cameras

Key Features

Features of school bus camera systems may include:

- Interior cameras
  - May record driver and students
- Exterior cameras (e.g., stop-arm cameras, dash cameras)
  - May record vehicles, pedestrians and driver
- Sound recording
  - May record driver and students
- Global Positioning System (GPS)
  - May record vehicle's location

Many capabilities are similar to video surveillance cameras

What's Unique?

School bus camera systems present different challenges from traditional video surveillance systems:

- Mobile devices pose additional challenges that impact on privacy
- Notifying individuals who may be recorded can be challenging
- The amount of data captured and storage location may pose security related problems

Implementing School Bus Camera Programs

Key Obligations under the Act

Legal Authorization

- Ensure the school board has the legal authority to collect, use and disclose personal information under *MFIPPA*
- Real, substantial, and pressing problem to be addressed and less privacy intrusive means are not feasible
- Video surveillance should always be a last resort

Data Minimization

- Limit the collection, use, retention and disclosure of personal information to that which is necessary for the purposes of the program

Cont'd

Key Obligations under the Act

Notice

- Notify the public prior to beginning the program
- Utilize local media, social media and the consortium and school boards' websites
- Post a notice on the rear window of the bus if external cameras (but ensure it does not contravene rules and regulations re: school buses)
- Post a notice inside the bus if internal cameras
- Ensure that the information required by *MFIPPA* s. 29(2)(a)–(c) is available and easily accessible on the consortium and school boards' websites

Cont'd

Key Obligations under the Act

Retention

- Limit retention of personal information to the amount of time reasonably necessary to discover or report an incident that occurred in the space under surveillance

Security

- Protect the personal information collected from unauthorized access and disclosure, and inadvertent destruction or damage
- Use strong encryption, and securely store information in transit and at rest
- Log and audit accesses and changes to the system

Cont'd

Key Obligations under the Act

Access Requests

- School boards must be prepared to process freedom of information requests from the public
- All or portions of the video footage requested may be exempt from disclosure under *MFIPPA*
- School boards must develop protocols for the redaction of personal information from the video footage where appropriate

Key Obligations under the Act

Access Requests (continued)

- School boards may use tools and techniques to redact personal information such as:
  - Digitizing analogue footage to enable the use of more powerful editing tools
  - Blacking out or blurring images of individuals
  - Removing the sound of voices

Access Example: TTC Footage

IPC Order MO-3238

- Request for bus surveillance tape pertaining to an incident that occurred on a Toronto Transit Commission bus
- Requester asked for copy of the tape to prove that he was assaulted by a bus driver
- TTC identified a surveillance tape, but denied access as it was considered an unjustified invasion of privacy
- Adjudicator disagreed and ordered footage to be disclosed after severing the personal information of other identifiable individuals

Access Example: City CCTV Footage

IPC Order MO-3358

- A reporter sought access to camera footage from five locations near the scene of a fatal collision between a bus and a train
- The city identified five clips of CCTV camera footage from certain locations that had images, most notably faces, that were blurred using image blurring technology, but denied access, citing an unjustified invasion of privacy
- IPC found CCTV camera footage with blurring technology applied would not invade privacy and it was ordered to be disclosed

Best Practices

Best practices for school boards implementing a school bus camera program include:

- Consulting your school board's Freedom of Information and Privacy Coordinator and the public
- Conducting a privacy impact assessment (PIA)
- Establishing policies and procedures
- Establish a privacy breach protocol
- Training employees
- Auditing roles, responsibilities, and practices
- Consulting with our office

Privacy Impact Assessments (PIA)

- A PIA is a formal risk management tool used to **identify the actual or potential risks** that a proposed or existing information system, technology or program may have on individuals' privacy
- A PIA should be conducted during the design phase and **prior to implementation**
- IPC **highly recommends** a PIA

Planning for Success:
Privacy Impact Assessment
Guide

Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario

Benefits of a PIA

A PIA will help:

- Identify privacy and security risks
- Develop mitigation strategies
- Reduce costs by providing “early warnings” of challenges
- Determine necessary roles and responsibilities
- Foresee problems in merging technologies and systems
- Set standards for new data handling practices and existing systems handling new information

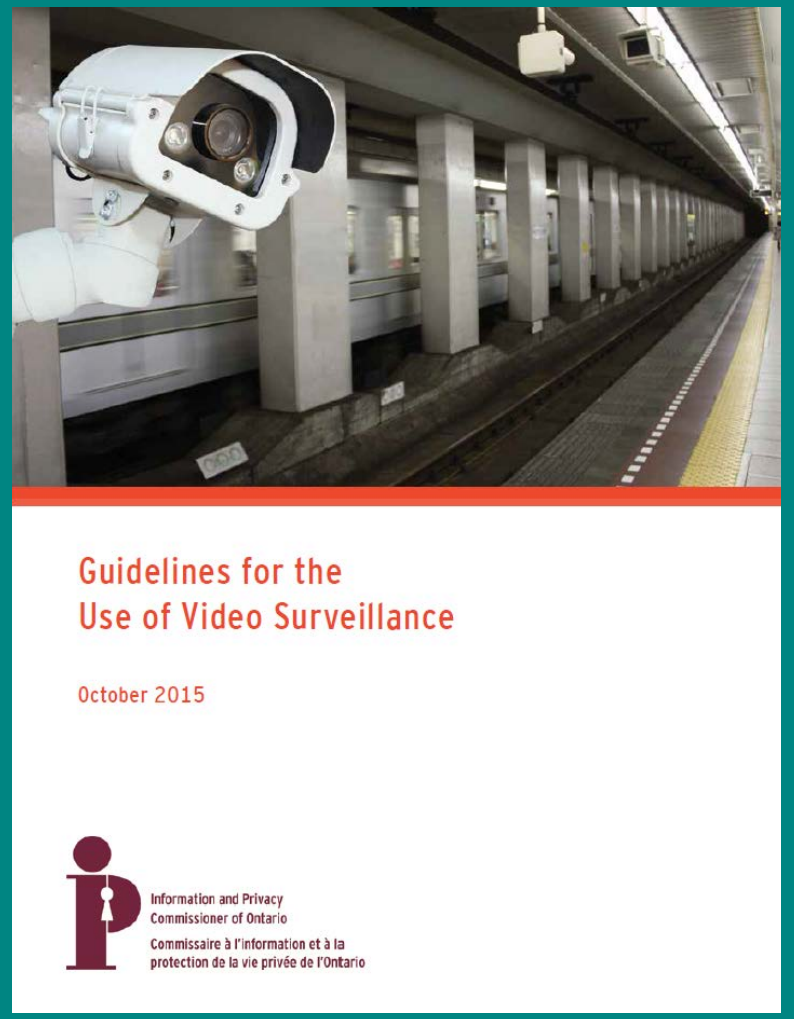
Policies and Procedures

Comprehensive policies and procedures should be in place to address privacy and security issues including:

- When recording will be permitted, required, or prohibited
- Retention, use, disclosure, and destruction of recordings
- Privacy/security safeguards for cameras, servers, and other systems (e.g. encryption, role-based access, and audit processes)
- Responding to access requests

Video Surveillance Guidelines

- The IPC published video surveillance guidelines in 2015 and a fact sheet in 2016
- These documents consolidate previous advice provided by the IPC, and present new issues and factors to consider, including **retention periods** and **notices of collection**
- They also provide **key messages** and **examples** for clarity



Police Body-Worn Camera Guidance

- Canada's federal, provincial, and territorial Commissioners issued guidance on police use of body-worn cameras in 2015
- Recommendations include conducting a PIA, providing notice to the public, and establishing comprehensive policies and procedures for using the cameras

GUIDANCE FOR THE USE OF
BODY-WORN CAMERAS
BY LAW ENFORCEMENT AUTHORITIES

This guidance document aims to identify some of the privacy considerations law enforcement authorities should take into account when deciding whether to outfit law enforcement officers with body-worn cameras. Also described is the privacy framework that should be part of any law enforcement body-worn camera program in order to ensure compliance with Canada's personal information protection statutes.

This document is endorsed by:

Office of the Privacy Commissioner of Canada
Office of the Information and Privacy Commissioner of Alberta
Office of the Information and Privacy Commissioner for British Columbia
Manitoba Ombudsman
Office of the Access to Information and Privacy Commissioner - New Brunswick
Office of the Information and Privacy - Newfoundland and Labrador
Office of the Information and Privacy Commissioner of the Northwest Territories
Nova Scotia Freedom of Information and Protection of Privacy Review Office
Office of the Information and Privacy Commissioner of Nunavut
Office of the Information and Privacy Commissioner of Ontario
Office of the Information and Privacy Commissioner of Prince Edward Island
Commission d'accès à l'information du Québec
Office of the Saskatchewan Information and Privacy Commissioner
Office of the Yukon Information and Privacy Commissioner

New Legislation Re: School Bus Cameras in Ontario

- Bill 174, the *Cannabis, Smoke-Free Ontario and Road Safety Statute Law Amendment Act, 2017,* was introduced on November 1, 2017 and received Royal Assent on December 12, 2017
- Schedule 4 of the bill amends the *Highway Traffic Act* to include:
  - New regulation making authority to prescribe requirements to support automated school bus camera systems, including evidentiary rules regarding evidence captured by the systems
  - Expands the current school bus passing offence to include when the stop arm is actuated, in addition to the existing requirement for overhead red lights to be flashing

Questions?

HOW TO CONTACT US

Information and Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073

TDD/TTY: 416-325-7539

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

Media: media@ipc.on.ca / 416-326-3965