FOIPN Fall Network Meeting

David Goodis

Assistant Commissioner

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

Freedom of Information Police Network Conference

October 26, 2017

Who is the Information and Privacy Commissioner?

- Brian Beamish appointed by Ontario Legislature (March 2015)
  - 5 year term
  - reports to Legislature, not government or minister
  - ensures independence as government “watchdog”

Mission and Mandate

MISSION: We champion and uphold the public's right to know, and right to privacy

MANDATE:

- resolve access to information appeals and privacy complaints
- review and approve information practices
- conduct research, deliver education and guidance on access and privacy issues
- comment on proposed legislation, programs, and practices

Legislation

IPC oversees compliance with:

Freedom of Information and Protection of Privacy Act (FIPPA)

- over 300 provincial institutions such as ministries, provincial agencies, boards, commissions, colleges, universities

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

- over 1,200 organizations such as municipalities, police, school boards, conservation authorities, transit commissions

Personal Health Information Protection Act (PHIPA)

- Individuals/organizations delivering health care, including hospitals, pharmacies, laboratories, doctors, dentists, nurses

Commissioner's Mandate

- Commissioner's tribunal role in access matters:
  - if government agency denies access to document, or gives only partial access
  - appeal to Commissioner, who can conduct inquiry, order agency to disclose document
  - order is final, unless judicial review (*JRPA*)

Commissioner's Mandate

- Commissioner's tribunal role in privacy matters:
  - investigate complaints about government breach of *MFIPPA* privacy rules
    - e.g. improper collection, use, disclosure of PI
    - can be on Commissioner's "own motion"
  - report with findings of fact and law, recommendations (no JR or appeal; Ombudsman-like role)
  - decisions = Ontario case law

MFIPPA overview

Purposes of *MFIPPA* are:

- provide a right of access to information held by institutions in accordance with the principles that,
  - information should be available to the public
  - access exemptions should be limited and specific
  - access decisions should be reviewed independently of government
- protect the privacy of individuals with respect to personal information about themselves held by institutions and to provide individuals with a right of access to their information

Principles of Access and Privacy

Access in Ontario

Under *MFIPPA*, every person has a **right** to access a record or part held by an institution unless:

- contents fall within exemptions [privacy, law enforcement]
- request is frivolous or vexatious
- record is specifically excluded [e.g., employment, ongoing prosecution]
- another act overrides [e.g., confidentiality provisions in *Municipal Elections Act*]

Right of access applies to almost any record including:

Correspondence	Working Notes (notebooks)	Photos
Memos	Expense Accounts	Videos
Emails	Appointment Books and Schedules	
Draft documents	Voicemails and Texts	

Requests

Requests can be made for any type of record, by anyone, with no obligation on the requester to provide a reason for making the request

Three types of requests:

- general information
- personal information
- correction

Once an access request is received **all responsive records must be retained** – they cannot be altered, deleted, or shredded

Exemptions: Limited and Specific

Two categories of exemptions under Ontario's access laws:

- mandatory exemption – institution *must* withhold the record
- discretionary exemption – institution *may choose* to withhold the record

DISCRETIONARY EXEMPTIONS

- draft by-laws, record of closed meetings
- advice or recommendations
- law enforcement
- economic interests
- solicitor-client privilege
- danger to safety or health
- information soon to be published

MANDATORY EXEMPTIONS

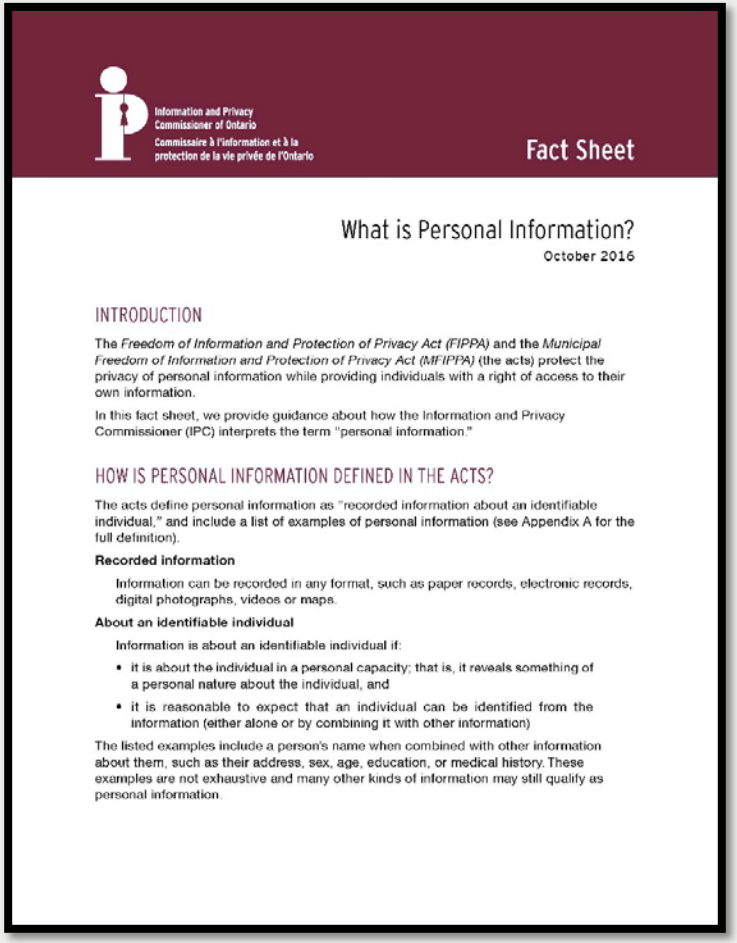
- relations with other governments
- third party commercial information
- someone else's personal information

Privacy and *MFIPPA*

MFIPPA establishes **rules for collection, use, 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

Personal Information



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.

- Personal information is **any recorded information that is identifiable to an individual**
- *MFIPPA* lists examples of personal information
- fact sheet provides guidance about how the IPC interprets the term "personal information"

Key Obligations under *MFIPPA*

- legal authority to collect
- data minimization
- notice to data subjects
- retention
- safeguards
- give person access to their own PI

Privacy Obligations Under *MFIPPA*

MFIPPA rules for **collection**, **use**, **disclosure**

To **collect**, must be:

- expressly authorized by statute
- used for purposes of law enforcement, or
- necessary to 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:

- purpose it was collected
- 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
- health and safety reasons
- compassionate reasons

Example:

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

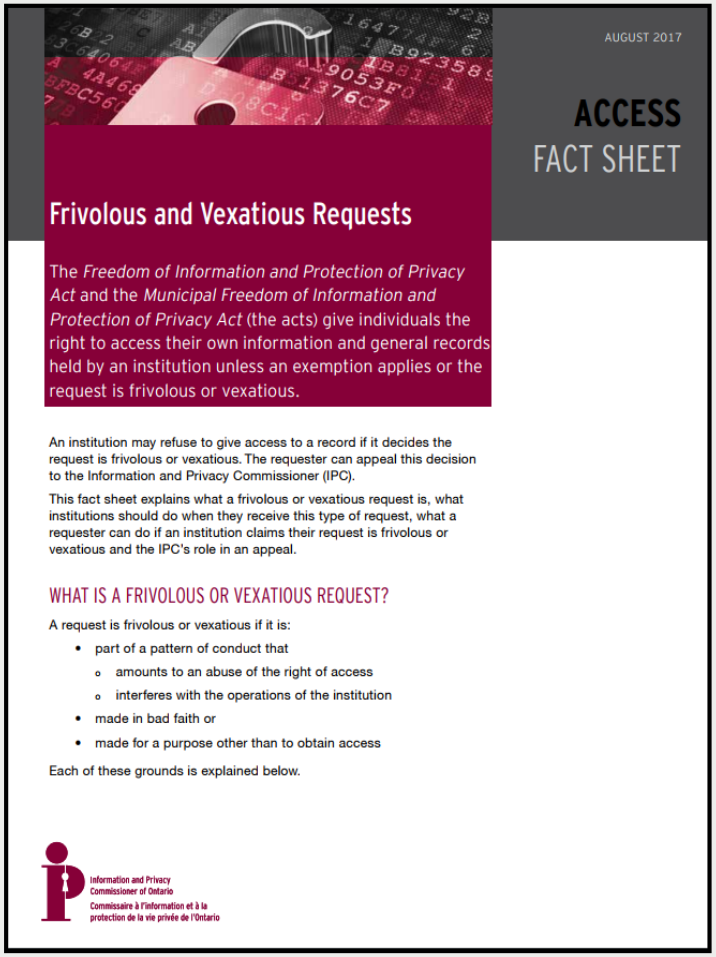
Access Risks

Frivolous and Vexatious Requests

An institution may refuse to give access to a record if request is frivolous or vexatious

A request is frivolous/vexatious if:

- part of a pattern of conduct that
  - amounts to an abuse of the rights of access
  - interferes with the operations of the institution
- made in bad faith or
- made for a purpose other than to obtain access



AUGUST 2017

ACCESS
FACT SHEET

Frivolous and Vexatious Requests

The *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act* (the acts) give individuals the right to access their own information and general records held by an institution unless an exemption applies or the request is frivolous or vexatious.

An institution may refuse to give access to a record if it decides the request is frivolous or vexatious. The requester can appeal this decision to the Information and Privacy Commissioner (IPC).

This fact sheet explains what a frivolous or vexatious request is, what institutions should do when they receive this type of request, what a requester can do if an institution claims their request is frivolous or vexatious and the IPC's role in an appeal.

WHAT IS A FRIVOLOUS OR VEXATIOUS REQUEST?

A request is frivolous or vexatious if it is:

- part of a pattern of conduct that
  - amounts to an abuse of the right of access
  - interferes with the operations of the institution
- made in bad faith or
- made for a purpose other than to obtain access

Each of these grounds is explained below.

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

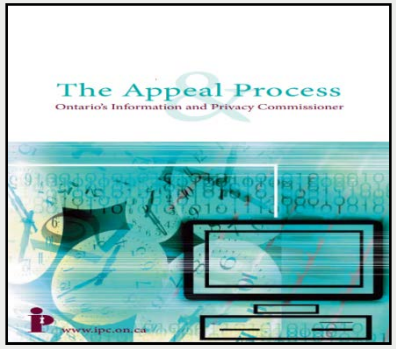
Challenging Requests

Requests that are not deemed frivolous or vexatious can still be challenging to process. Institutions can take certain steps to help manage such requests:

- publish records disclosed in response to FOI requests on website (subject to privacy concerns)
- develop policies to enable proactive disclosure
- work with requester to focus or clarify the request, and document all attempts to clarify in writing
- apply fee provisions of the act
- apply time extension provisions of the act

Appeals and Mediation

Any person has a right to file an appeal with the IPC to request a review of a government institutions decision regarding an access request



Three stages in appeal process:

1. Intake
2. Mediation
3. Adjudication

At mediation, parties have chance to explain their respective positions, issues are clarified, options are generated, and agreements negotiated

Mediation helps to build trust, understanding and communication between parties and thereby improves future interactions

Most IPC appeals resolved during the mediation

Contentious Issues Management

IPC has said that a contentious issues management system designed to give senior officials a heads up about the disclosure of potentially controversial records is **acceptable**

However, such a system should **never interfere** with the statutory timeframe for responding to access requests, and the appropriate processing of such requests

The process can be used as a way to prepare and assist senior officials when responding to questions from the media or the general public about a particular issue

In 2011, the IPC investigated the issue at the Ontario Ministry of Finance, and issued the *Report Into Contentious Issues Management in the Ministry of Finance*

Privacy Risks

Common Privacy Breaches

1. Insecure disposal of records
   - records in paper format intended for shredding are recycled
   - insecure disposal of hard drives
2. Mobile and portable devices
   - lost or stolen, unencrypted devices such as laptops, USB keys
3. Unauthorized access
   - snooping by otherwise authorized staff, malware (e.g. ransomware)

Snooping into records

- if privacy not built into the **design and implementation** of records management processes, it can pose unique and challenging **risks** to privacy, such as an increase in risk of unauthorized individuals accessing personal health information

Harms caused by personal information snooping:

- discrimination, stigmatization, psychological or economic harm
- individuals withholding or falsifying information
- loss of trust or confidence in the public system
- cost and time in dealing with privacy breaches
- legal liabilities and proceedings

Sanctions for unauthorized access can include:

- investigation by privacy oversight bodies
- prosecution for offences
- statutory or common law actions
- discipline by employers
- discipline by regulatory bodies

Toronto Police Service (MC-030009-1)

IPC received a complaint under *MFIPPA* relating to two occurrence reports about the complainant, who claims reports were improperly retained by a detective when he retired

IPC investigation found **no authority** under *MFIPPA* that would permit the detective to remove and retain copies of police records containing the personal information of others for his/her own personal use after his retirement

IPC advised the TPS to take all necessary steps to recover copies of the occurrence reports and any other records the detective may have retained

Ministry of Community Safety and Correctional Services (PC11-34)

IPC receives complaint that OPP staff inappropriately disclosed an occurrence report to the complainant's landlord which included her personal information

IPC finds that disclosure of the report was not in accordance with s. 42(1) of *FIPPA* which provides a general prohibition against the disclosure of personal information; none of exceptions applied

IPC recommended that a training program be developed which would require all clerical staff to undergo privacy training at regular intervals

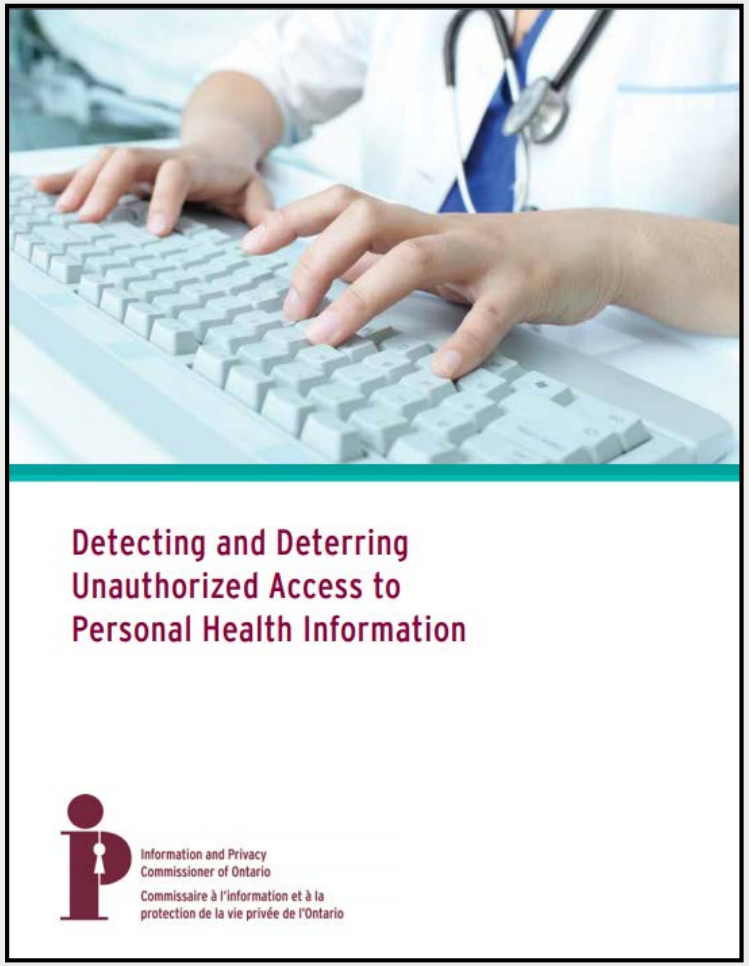
Rouge Valley Hospital (Order HO-013)

- two staff gathered “new baby” information, sold to RESP providers
- hospital had deficient audit measures to detect, deter snooping
- IPC ordered hospital to upgrade its systems to permit auditing, detection of snooping
- Rouge Valley appeals to Divisional Court
- first ever appeal of IPC health decision…but matter settled on hospital’s agreement to address system deficiencies

Reducing the Risk of Snooping

- clearly articulate the purpose for which employees, staff, and other agents may access personal information
- provide ongoing training and use multiple means of raising awareness such as:
  - confidentiality and end-user agreements
  - privacy notices and privacy warning flags
- where snooping discovered:
  - immediately terminate access pending an investigation
  - implement appropriate access control and data minimization
  - impose appropriate discipline for unauthorized access

Guidance on Snooping



- Reducing the risk through:

  - ✓ Policies and procedures
  - ✓ Training and awareness
  - ✓ Privacy notices and warning flags
  - ✓ Confidentiality and end-user agreements
  - ✓ Access management
  - ✓ Logging, auditing and monitoring
  - ✓ Privacy breach management
  - ✓ Discipline

CrimeReports' Crime Mapping Services

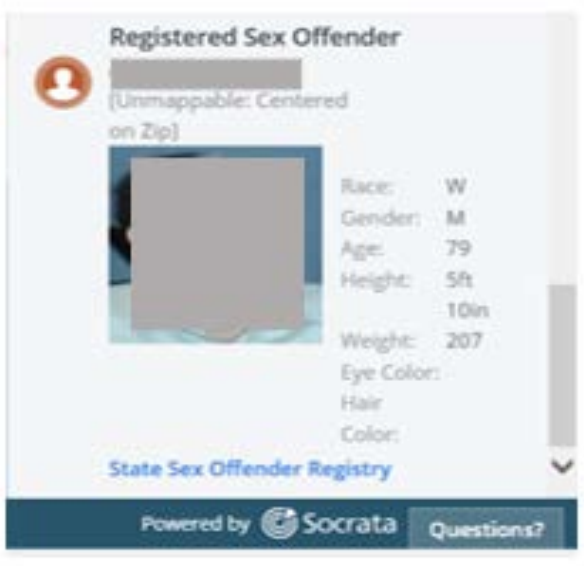
CrimeReports, offered by Motorola Solutions, provides a free subscription service that publishes crime data supplied by police services to an online map

This visualization tool enables the public to access and browse crime information from any computer or mobile device

Sex Offender Information

By default, CrimeReports' maps include information about US registered sex offenders residing in Ontario

Displayed are: photos, names, addresses, race, gender, age, height, weight, eye and hair colour



IPC Concern and Recommendation

Use of a crime mapping tool that displays the personal information of US sex offenders residing in Ontario may violate laws restricting disclosure of registered sex offender information [e.g., *Christopher's Law (Ontario Sex Offender Registry*), federal *Sex Offender Information Registration Act*]

IPC recently wrote to OACP asking for their assistance in making this issue known to Ontario police services

Recommendation: if police service contemplating using CrimeReports or comparable service:

- carefully review the functions of the crime mapping tool
- fully understand what personal information it collects, uses and discloses including data you are not providing
- work with the service providers to ensure sex offender information is not displayed or linked

Police Record Checks

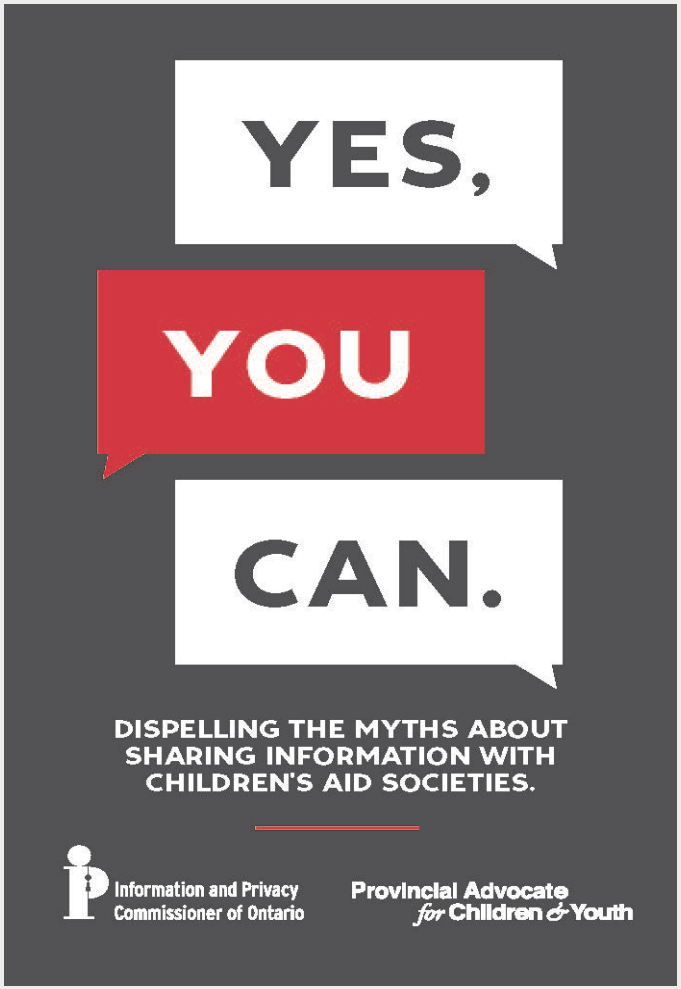
- problem across Canada that police background checks for employment, volunteer positions inconsistent
- sometimes non-conviction (including mental health) information disclosed without justification
  - IPC Crossing the Line report
  - attempted suicide on CPIC due to 911 call
  - US border officials have direct, instant access

Police Record Checks

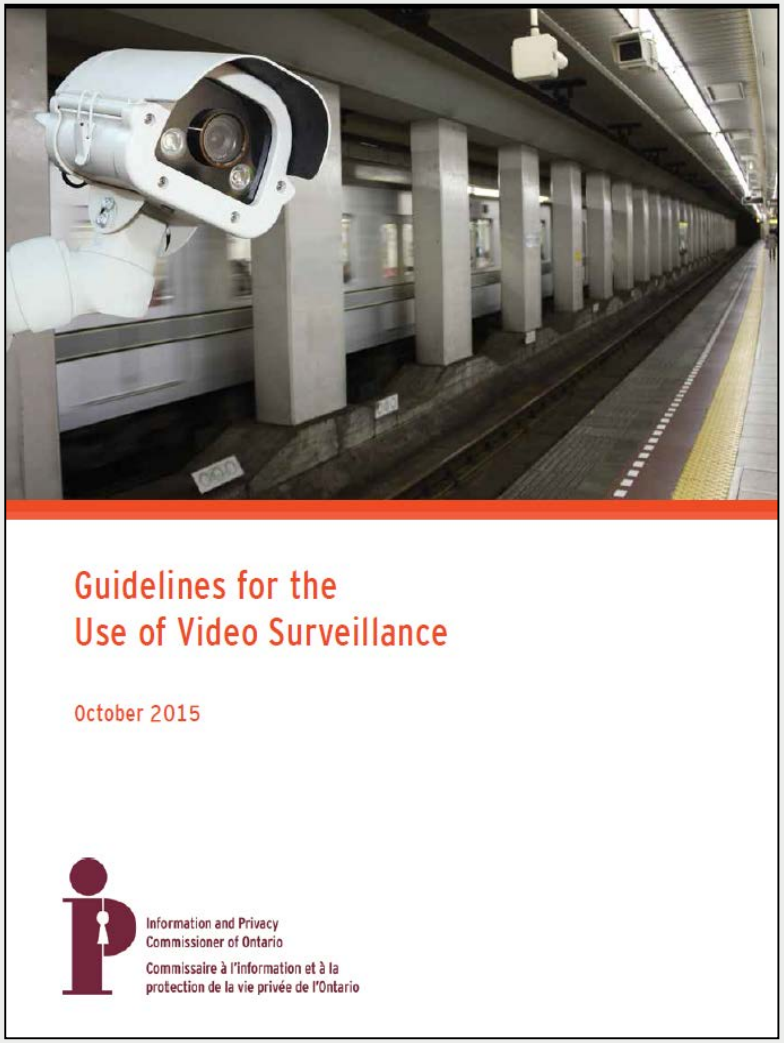
- *Police Record Checks Reform Act* [not yet in force]
  - 1st in Canada; based on OACP guidelines
  - 3 types: criminal record, criminal record and judicial matters, vulnerable sector
  - statute states precisely what information can be disclosed in each
  - non-conviction information disclosed only in vulnerable sector check, only if it meets "exceptional disclosure" test

Yes, You Can

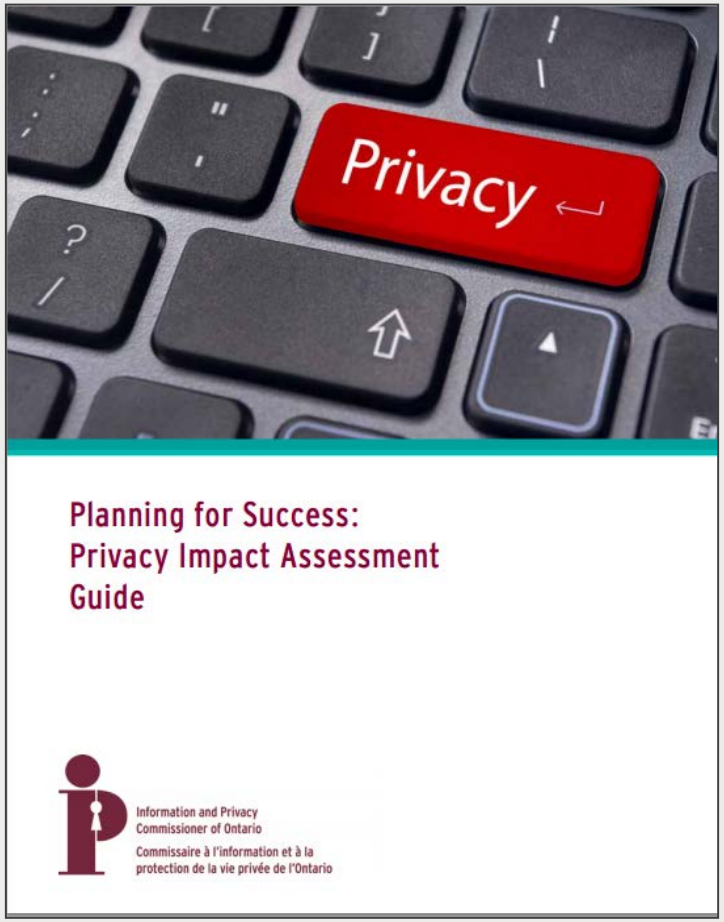
- IPC collaborates with Provincial Advocate for Children and Youth on guide about privacy and children's aid societies
- dispels myths, explains privacy legislation not a barrier to sharing information about a child who may be at risk [see *CFSA*]
- aimed mainly at school, police, social services, health care staff



Privacy: Video Surveillance Guidelines



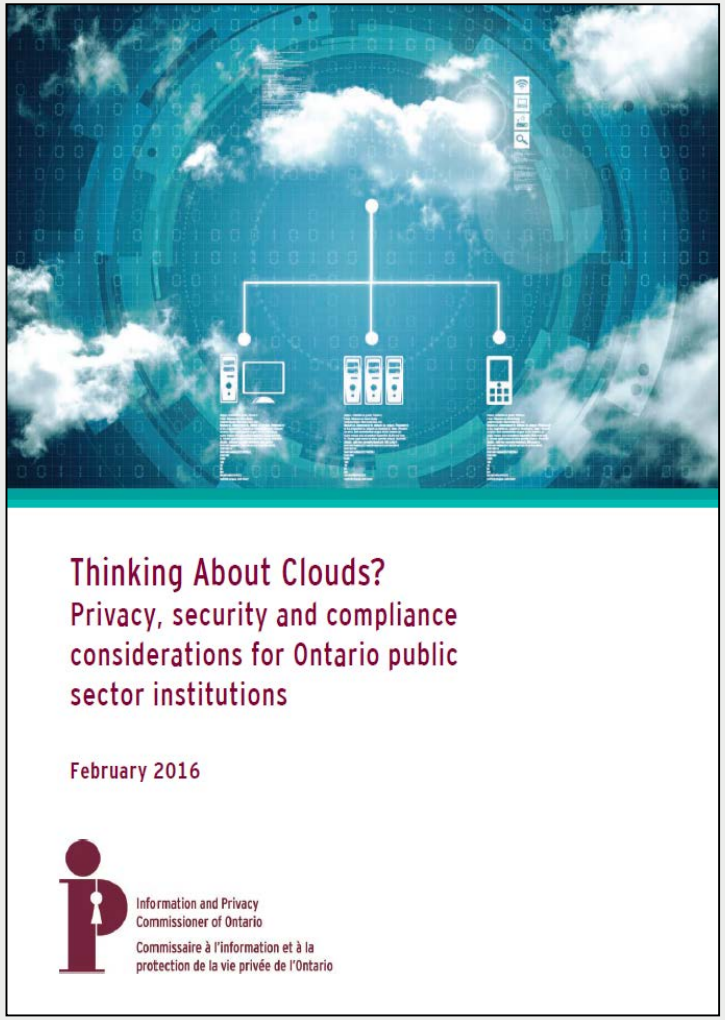
Planning for Success: Privacy Impact Assessment Guide



- tools to identify privacy impacts and risk mitigation strategies
- step-by-step advice on how to conduct a PIA

Thinking About Clouds?

- evaluate whether cloud computing services are suitable
- identify risks associated with using cloud computing
- outline strategies to mitigate risks
- aimed to assist smaller organizations



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