

Access and Privacy Update

**Frank DeVries, Manager of Adjudication
and Senior Adjudicator**

Renee Barrette, Director of Policy

Information and Privacy Commissioner of Ontario

**AMCTO Zone 9 Meeting
September 20, 2017**



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

Agenda

- Introduction
- Tribunal Department
 - The Appeal Process
 - Recent Orders of Interest to the Municipal Sector
 - Privacy and the Complaint Process
- Policy Department
 - Access and Privacy Tools and Guidance
 - New Challenges
 - Legislative Reform
- Questions



The Three Acts

The IPC oversees compliance with:

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

The purposes of MFIPPA and FIPPA are:

- to provide a **right of access to information** under the control of 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
- to **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 that information



The Appeal Process



Three stages of the appeal process

- **Intake**

Registrar oversees the intake stage of the appeal and complaint processes, and has the authority to direct files into different dispute resolution and adjudicative streams

- **Mediation**

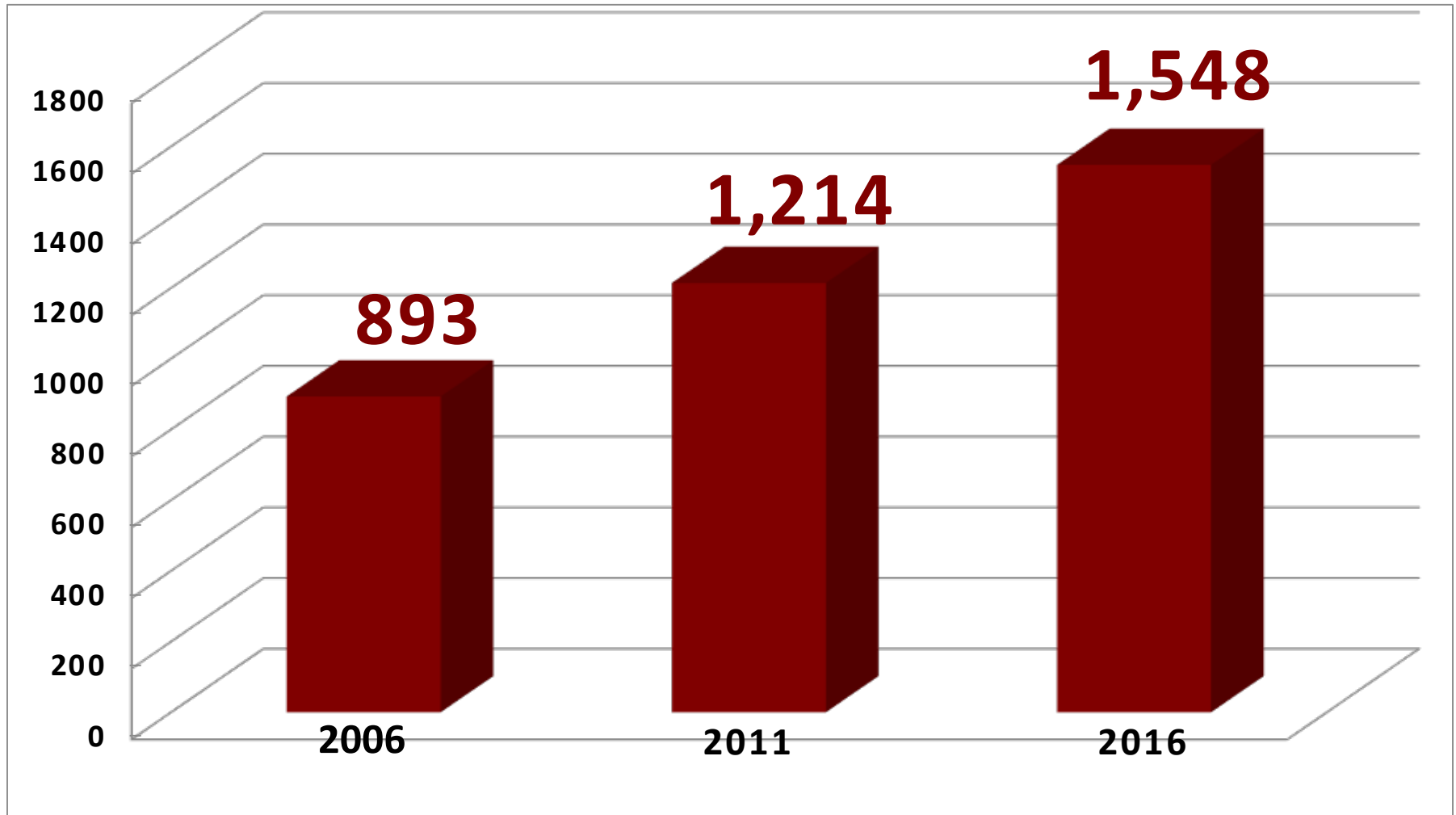
Mediators attempt to settle all issues in the appeal or, if not settled, narrow and clarify the issues that proceed to adjudication

- **Adjudication**

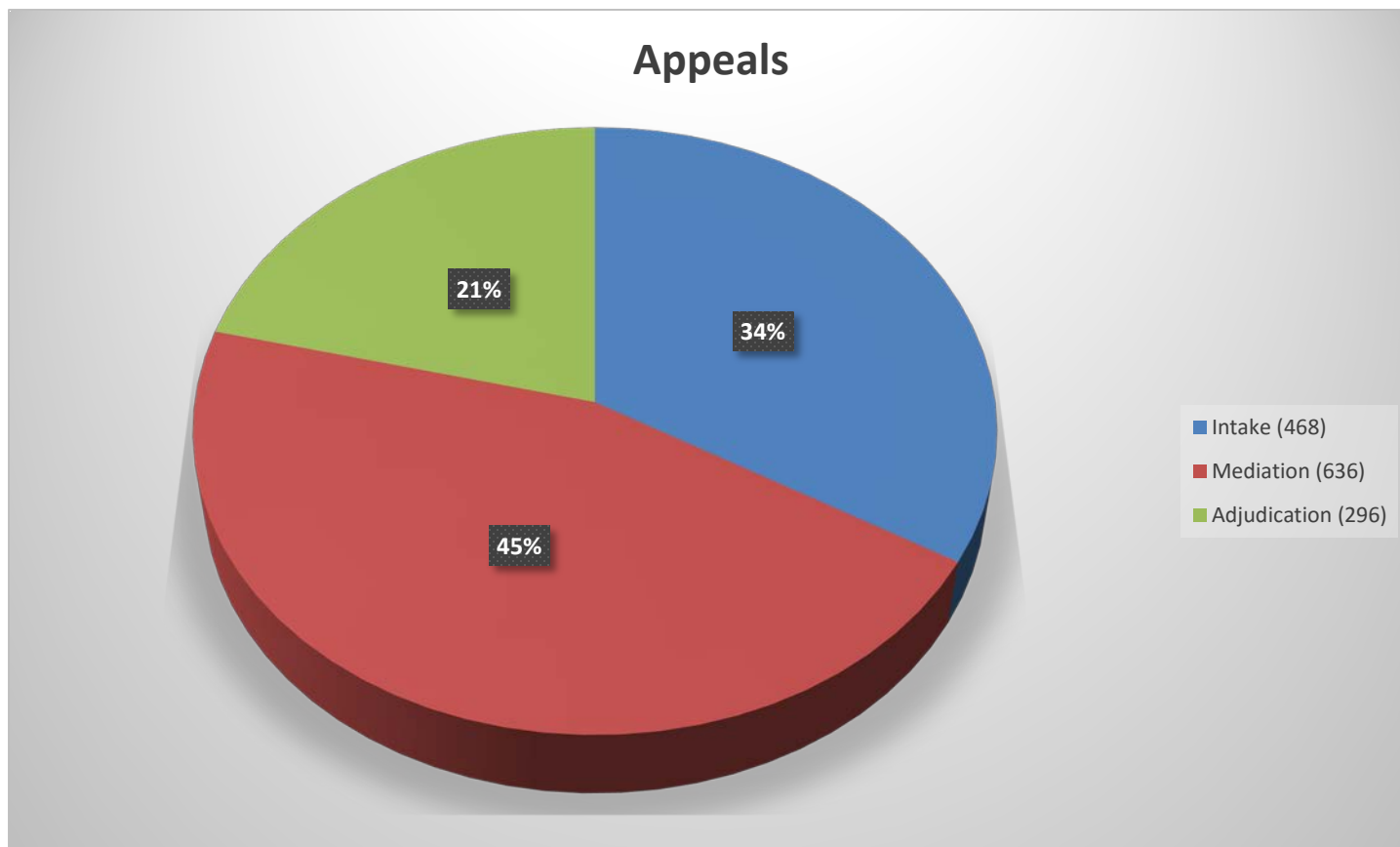
Adjudicator conducts an inquiry (usually in writing) to dispose of the issues in the appeal by issuing an Order.



Total Appeals Received Per Year



1,400 Appeals Closed in 2016



Intake Analyst Role

- Public Contacts – mail, phone and in-person
- Screen out appeals and privacy complaints
- Issue Order in Deemed Refusal and Failure to Disclose appeals
- Appeals – clarify, interim notice, screen out, resolve
- Privacy – clarify privacy issues, contact institution, consent, Intake Resolution Stream, Screen out
- Prepare memo for Registrar to move file to the investigation stream
- Analyst generally don't narrow or mediate appeals, except in Deemed Refusal and Failure to Disclose appeals



Intake - Screening

- Registrar, Team Leader and Analysts have delegated authority to screen out files where:
 - (a) The matter, on its face, is not within the IPC's jurisdiction (e.g. records from Royal Bank) or
 - (b) The matter falls within the IPC's jurisdiction, but the matter, on its face, is one that the IPC believes should not proceed through the appeal process (e.g. employment-related, prosecution, decided before, out of time)



Role of Mediator

The goal of the Mediator is to assist the parties:

- To clearly understand the appeal process and the issues in dispute
- To reach a voluntary, mutually acceptable resolution of some or all issues in dispute
- To clarify the issues and reduce the number of records and exemptions at issue
- Notify affected parties
- Provide advisory opinions based on past orders
- To explore interest-based and rights-based approaches



Advantages of Mediation

- Parties can explain their respective positions
- Parties retain control over the outcome
- Issues are clarified, options generated, common ground discovered and agreements negotiated
- Quicker and less costly
- Results in a win-win settlement that might not be possible through adjudication
- Builds trust, understanding and communication between parties and thereby improves future interactions



How to Ensure a Successful Mediation

- Prepare an Index of Records
- Respond to the mediator in a timely fashion and provide realistic deadlines
- Make an effort to understand the request, the appellant's real interests and the proposals
- Provide background explanations – be prepared to discuss the general nature of the records and the reasons why they are being withheld
- When participating in a teleconference, try to include the program area
- Ensure that decision makers are available to make decisions at the appropriate time
- Give due consideration to the mediator's advisory opinion



Files Processed at Mediation in 2016

- Fully Settled: **620** (64.5%)
 - No Issues Mediated: **163** (17.0%)
 - Partly Mediated: **162** (16.9%)
 - Abandoned: **15** (1.6%)
 - Withdrawn: **1** (0.1%)
- **Total files processed: 961 (100%)**



Adjudication

- Generally, an inquiry involves an Adjudicator soliciting written representations from the parties on the issues in the appeal, one party at a time
- Representations from one party are shared with other parties to the appeal unless there is an ***overriding confidentiality concern***
- The Adjudicator issues a binding Order disposing of the issues in the appeal



Inquiry

- 1st party Notice of Inquiry (NOI) sets out the facts and issues in the appeal and seeks representations from the party who bears the onus of proof (usually the institution)
- Adjudicator decides whether to invite representations from the second party. If so, the second party (usually the appellant) is also invited to make representations in response to the same or a modified NOI, and is provided with a copy of first party's non-confidential representations
- In some cases, the Adjudicator may send a further NOI to the first party, along with a copy of the second party's non-confidential representations, seeking their reply submissions
- Following these steps, an Adjudicator will issue an Order



Content of Representations

- Effective representations:
 - Address all of the issues identified in the NOI thoroughly and completely;
 - Highlight the confidential portions which are to be severed from the version that is shared with the other party, providing reasons for each severance that connect to the confidentiality criteria in the Code;
 - Provide supporting affidavits sworn by knowledgeable individuals where necessary; and
 - Avoid actual names (use affected person, accused etc).



Reconsideration of a Decision

- Section 18 of the IPC Code of Procedure sets out the criteria for reconsideration of an order or other IPC decision. The party seeking reconsideration must establish:
 - A fundamental defect in the adjudication process;
 - Some other jurisdictional defect in the decision; or
 - A clerical error, accidental error or omission or other similar error in the decision;
- The IPC will not reconsider simply on the basis of new evidence being provided.



Recent Orders of Interest to the Municipal Sector



PO-3695

Personal/professional distinction

- Access request made to the institution to disclose the name of a requester who had filed an earlier access request
- Institution notified the affected party (the person who made the earlier request) and, after hearing from them, decided to disclose their name on the basis that the affected party had not made the request in their personal capacity, and that it was therefore not personal information
- The affected party appealed



PO-3695 (cont'd)

- Applying the two-step analysis from PO-2225 for determining whether information is personal or professional, the adjudicator found that the name did not constitute “personal information”
- Applying step one of the analysis, she found a professional context to the name
- “... The evidence before me leads me to conclude that the appellant filed their access request as an individual acting for their own business interests as a professional who at the time of the request, carried on business at their residence”



PO-3695 (cont'd)

- With respect to whether disclosure would reveal something of a personal nature about the individual for the purpose of step two of the analysis, the adjudicator found that it would not
- The name of the individual who made the earlier access request was therefore ordered disclosed
- Note:
 - the analysis is contextual
 - the affected party was notified and involved in the process
- See also **MO-3310** (complaint made in professional capacity)



MO-3420

Personal/professional distinction

- Request for the names of municipal election candidates connected with information regarding election sign removal fees they incurred
- The information is ordered disclosed, as this information is about the election candidates in their official capacity, and is not personal information under section 2 of the *Act*
- Also applied the two-step analysis from PO-2225:
 - *In what context does the information appear?*
 - *Would disclosure reveal something that is inherently personal in nature?*



MO-3420 (cont'd)

- “In being held liable under the town’s bylaw for election sign removal costs, the town makes candidates responsible for the conduct of their election campaign, which is the official context in which registered election candidates operate. Consequently, I find that the withheld information relates to an official context”
- “... the withheld information in the spreadsheets and the invoices would not disclose information that would reveal something of a personal nature or that is inherently personal in nature”
- Note: notice given to all parties



MO-3370

Personal Privacy Exemption in section 38(b)

- Request made for the name and address of the owner of a dog that bit the appellant, contained in a file from Animal Services (records included an *Animal Incident Report* and *Rabies Incident Report*)
- The name and address of the affected party is ordered disclosed, as it is not exempt under the personal privacy exemption in section 38(b)



MO-3370 (cont'd)

- “I find that the factors favouring disclosure in sections 14(2)(b) (promote public health and safety) and (d) (fair determination of rights), as well as the unlisted factor (that the *Act* should not be used in a way that prevents individuals from exercising their legal rights), outweigh the privacy rights of the affected person concerning disclosure of her name and address”
- Note: the adjudicator found that the presumption in section 14(3)(b) did not apply to these records




MO-3370 (cont'd)

The adjudicator also considered:

- the city's revised position during the appeal to disclose the name
- the appellant's statement that the affected person provided her details to the relevant authority in her presence right after the bite incident
- that disclosure of the affected person's name and address is necessary to proceed with any potential claim in this matter
- the lack of representations from the affected person in response to the Notice of Inquiry, and
- the ability of the appellant to obtain this information under Rule 30.10 of the *Ontario Rules of Civil Procedure*



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**
- The acts list examples of personal information
- This fact sheet provides guidance about how the IPC interprets the term "personal information"



Custody and control

General approach from previous orders:

- There are numerous listed factors to consider in deciding whether records are in the custody or control of the city (ie: who created records, why, core function of city, regulate use and disposal, etc.)
- SCC two-part test in *National Defence*, on whether an institution has control of records that are not in its physical possession:
 - (1) Do the contents of the document relate to a departmental matter?
 - (2) Could the government institution reasonably expect to obtain a copy of the document upon request?
- See decision in *City of Ottawa* [2010 ONSC 6835 (Div. Ct.)]



MO - 3471

Custody and control – councillor records

- Request made to the City of Toronto for access to communications sent or received by the staff of a named councillor relating to the councillor's Twitter account
- The city denied access to any responsive records that might exist on the basis that it does not have custody of or control over the records within the meaning of section 4(1) of the *Act*
- The adjudicator upheld the city's decision



MO-3471 (cont'd)

- Representations were sought from the city, the councillor and the appellant
- The adjudicator reviewed the listed factors in deciding whether records are in the custody or control of the city
- Found the request was for communications within the councillor's office (not between the councillor's staff and city staff)
- Structure of roles of councillor and staff (from city handbook) support a finding that a councillor's entire office, including its staff, is distinct from the offices of the city as an institution



MO-3471 (cont'd)

- Found the councillor was not acting as an officer or employee of the city when the records, if they exist, were created. As well, his staff, though city employees, are not part of the public service (they assist councillor in his role as an elected representative)
- Found no "unusual circumstances" such that the councillor should be considered an officer of the city
- Also considered the SCC two-part test:
- (1) Do the contents of the document relate to a departmental matter?
- (2) Could the government institution reasonably expect to obtain a copy of the document upon request?



Other orders

- MO-3281 - found that an email from a City of Oshawa councillor to an investigator who was later hired by the city was in the city's control because the city had the authority, when directed by council, to retain an investigator, and because the creation of the record at issue played an integral part in council's decision to retain the investigator.
- MO-3450 – upheld the Town of Kapuskasing's decision that the audited financial statements of the Federation of Northern Ontario Municipalities are not in the town's custody or under its control for the purposes of the Act.



Councillors' Records



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

FOI Fact Sheet 1

The *Municipal Freedom of Information and Protection of Privacy Act* and Councillors' records

April 2016

INTRODUCTION

The Information and Privacy Commissioner of Ontario (IPC) sometimes decides appeals relating to requests for access to records created or held by municipal councillors. The *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* does not expressly refer to records of municipal councillors and, therefore, before a determination can be made on access to those records, the IPC must decide whether *MFIPPA* applies. In making this decision, the IPC examines the specific facts of each case in light of a number of principles.

The IPC has been calling for amendments to *MFIPPA* to clarify when it applies to these records, including in August 2015, when the IPC wrote to the Minister of Municipal Affairs and Housing setting out proposed amendments (this letter is available on the IPC's [website](#)).

In the absence of amendments, however, the IPC is issuing this fact sheet, which explains when and how councillors' records are subject to *MFIPPA*.

WHEN ARE COUNCILLORS' RECORDS SUBJECT TO *MFIPPA*?

Councillors' records are subject to *MFIPPA* where:

1. a councillor is acting as an officer or employee of the municipality, or performs a duty assigned by council, such that they might be considered part of the institution, or
2. the records are in the custody or control of the municipality.

WHEN IS A COUNCILLOR AN OFFICER OR EMPLOYEE OF A MUNICIPALITY?

A councillor is likely to have several roles, such as an individual constituent representative, a politician, or a head or member of a municipal committee or board, such as a transit corporation. Some of these roles may entail the councillor acting as an officer or employee, while others do not.

- Determining whether *MFIPPA* applies to councillors' records depends largely on context and involves considering of a number of factors
- This fact sheet explains when and how councillors' records are subject to *MFIPPA*.



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

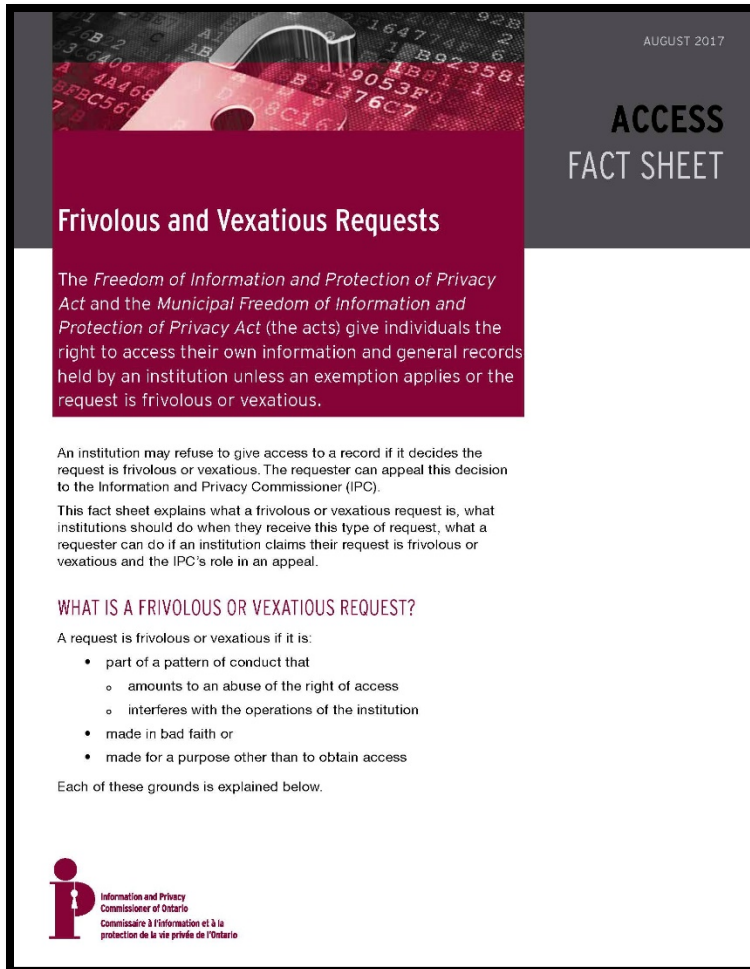
Other orders

Frivolous or vexatious requests

- PO-3691 - the adjudicator finds that the number of requests submitted by the appellant amounts to a pattern of conduct that interferes with the operations of the institution, and that the requests are “frivolous and vexatious” for the purpose the *Act* and the applicable Regulation. The appellant is restricted to five active requests at any given time
- See also Order MO-3049



Frivolous and Vexatious



- A request is frivolous or vexatious if it is made:
 - As part of a pattern of conduct that amounts to an **abuse of the right of access** or **interferes with the operations of the institution**
 - In **bad faith** or
 - For a **purpose other than to obtain access**
- This fact sheet provides guidance on frivolous and vexatious requests, including specific IPC Orders regarding such requests

Interim Order MO-3395-I

Third party information

- A request was made for access to records relating to the town's decision to provide a \$2.8 million loan to a local soccer club
- The adjudicator found that the exemption in section 10(1) (third party information) did not apply to the records
- The denial of access to one record under the closed meeting exemption is upheld



MO-3395-I (cont'd)

- Applying the three-part test in section 10(1), the adjudicator found:
 - a clause in the loan agreement cannot qualify as having been “supplied” by the third party because it was mutually generated between the parties
 - the town and the third party failed to establish that the prospect of disclosing the third party’s financial information in the records at issue will give rise to a reasonable expectation that the harms specified in paragraphs (b) and (c) of section 10(1) will occur.



Other orders

Third party information

- MO-3376 - a city's decision to grant access to copies of the successful proposal relating to the city's purchase of refuse packers, as well as any contract and/or purchase orders relating to it, is upheld, and the information is ordered disclosed
- MO-3372 specific pricing information in invoices that a waste management company sent to the city is not exempt from disclosure under section 10(1) (third party information), and the city is ordered to disclose it



Other orders

Third party information

- PO-3598 - an agreement between the university and a bank relating to the issuance of university-branded credit cards does not qualify for exemption under section 17(1) (third party information) because the information was not supplied by the third party.
- This decision was upheld on Judicial Review (*Toronto-Dominion Bank v. Ryerson University*, 2017 ONSC 1507).
- Request for leave to appeal to the Ontario Court of Appeal was denied.



Privacy and the Complaint Process



Privacy Obligations under *MFIPPA*

Collection, use, disclosure rules

No **collection** unless

- authorized by statute
- used for law enforcement or
- necessary to lawfully authorized activity

Must have a legitimate reason for collecting personal information, such as requiring a birth certificate to issue a driver's license

No **use** unless

- purpose collected
- consistent purpose
- written consent

Cannot use information from the birth registry to send out birthday cards

No **disclosure** unless

- consent
- consistent purpose
- comply with legislation
- law enforcement
- health or safety
- compassionate reasons

Video capturing evidence of a crime can be shared with police, even if it contains personal information



Privacy Complaints

- Ontario's freedom of information **acts help protect personal information** held by provincial and local government organizations: it is the responsibility of the IPC to ensure that government organizations abide by the acts
- The IPC may **investigate privacy complaints**, report publicly on them
 - may order government to cease and destroy a collection of personal information
 - may make recommendations to safeguard privacy
- The Registrar will stream a privacy complaint to the **intake resolution stream** if it appears that a quick informal resolution can be achieved without having to go through a formal investigation



Privacy Complaints

Investigation Stream

- The Registrar will stream all other privacy complaint files to the investigation stream
- An Investigator will be assigned to:
 - **Clarify** the complaint
 - Contact the parties, **gather information**, attempt settlement
 - Make findings and issue a **Privacy Complaint Report** with orders and/or recommendation
 - Default is a public report



Privacy Complaints

Stats for FIPPA/MFIPPA

- Complaints opened in 2016: **277**
- Complaints closed in 2016: **273**
 - Resolved: **165** (64.5%)
 - Screened-out: **59** (23%)
 - Withdrawn: **27** (10.5%)
 - Abandoned: **3** (1.2%)
 - Report: **2** (0.8%)



Policy Department



Information and Privacy
Commissioner of Ontario

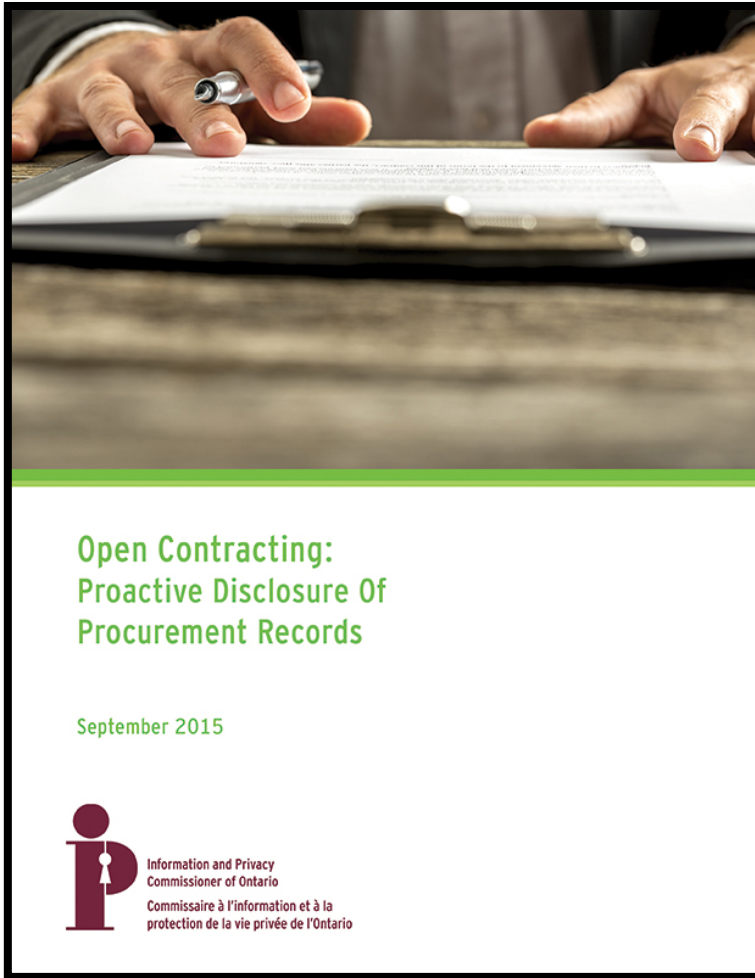
Commissaire à l'information et à la
protection de la vie privée de l'Ontario

IPC's Policy Role

- Engage in **research** into matters affecting the purposes of the acts
- **Comment** on proposed legislative schemes or government programs
- **Educate** the public and stakeholders about Ontario's access and privacy laws, and access and privacy issues through research, publications and public speaking
- Develop **guidance** to help institutions understand their legislative obligations and how to appropriately address access and privacy issues and help the public understand their access and privacy rights



Open Contracting



- Proactive disclosure of procurement records improves the **transparency of government spending** and reduces resources required to respond to access to information requests
- This paper provides guidance on how to make procurement records publically available, while protecting sensitive **third party information** and **personal information**

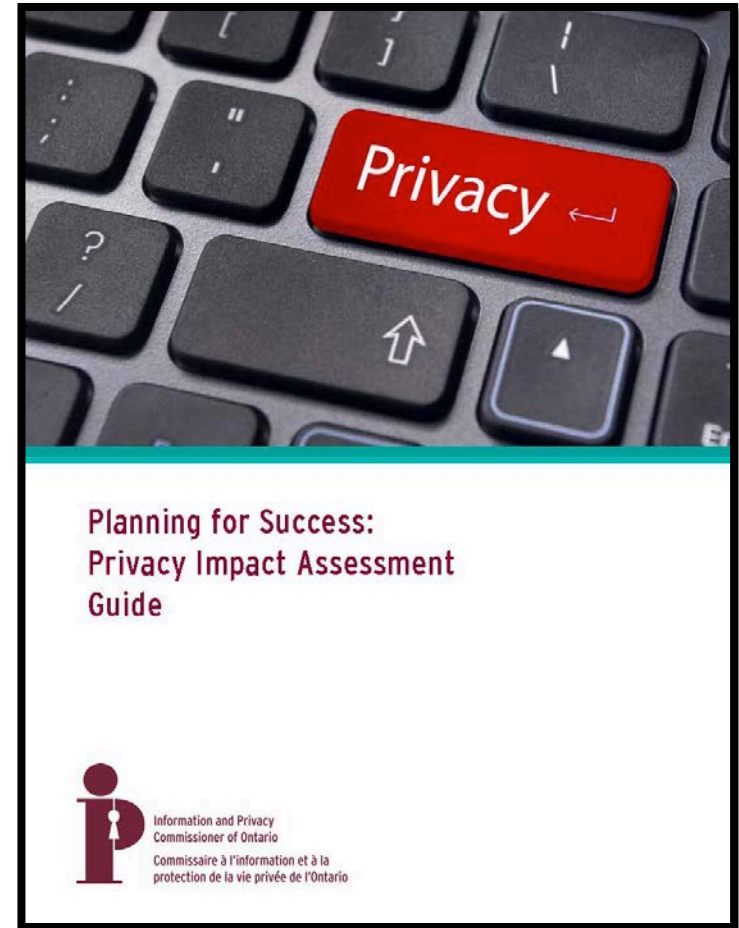
Open Contracting

- Open contracting has a number of benefits including:
 - Improved public confidence and trust
 - Increased accountability on spending
 - Increased fairness and competition in contracting
 - Reduction in the number of access to information requests and appeals
- An open by default approach to procurement records can be achieved by:
 - **Designing with transparency in mind:** Make proactive disclosure the default
 - **Engaging stakeholders:** Ensure they are informed and understand the process from the outset
 - **Creating searchable records:** The public must be able to search for records in intuitive and user-friendly ways
 - **Explaining limited exceptions:** Clearly define the reasons why information will not be published



Privacy Impact Assessment Guide

- PIAs are tools to identify privacy impacts and risk mitigation strategies
- Widely recognized as a **best practice**
- Benefits of a PIA:
 - **Risk mitigation** - Best tool to identify privacy risks, document countermeasures and implement mitigation strategies
 - **Ethical** - Transparent PI handling practices
 - **Compliance** - directives, policies, legal and legislative requirements
 - **Save time and money** - avoid re-designs, delays, risk of project cancellation



Privacy Impact Assessment Guide

PIA Methodology and Tools

Key Steps	Tools
1. Preliminary Analysis Is personal information involved?	Appendix A: Questionnaire
2. Project Analysis Gather project info, people and resources	Appendix B: Questionnaire
3. Privacy Analysis Identify and mitigate risks	Appendix C: Checklist
4. PIA Report Document findings, get approval, proceed	Appendix D: Template

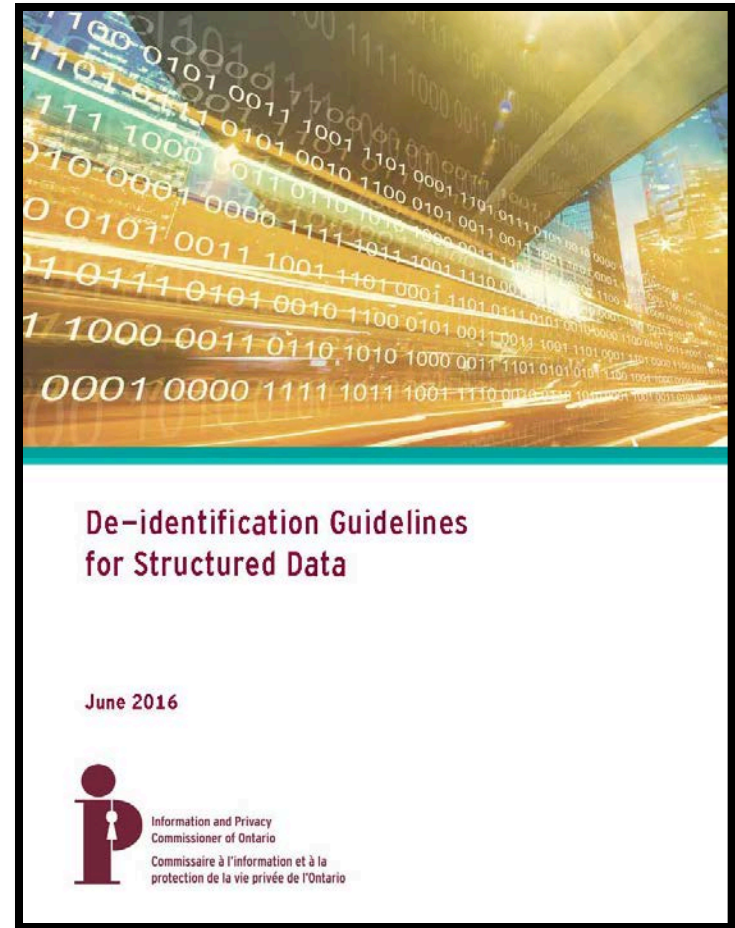
Downloadable Worksheet containing all Appendices:

https://www.ipc.on.ca/wp-content/uploads/2016/11/planning-for-success-pia-guide_worksheets.rtf



De-identification Guidelines for Structured Data

- De-identification is the removal of personal information from a record or data set
- This guide outlines a risk-based, step-by-step process to assist institutions in de-identifying data sets containing personal information
- Covers key issues to consider when publishing data:
 - Release models
 - Types of identifiers
 - Re-identification attacks
 - De-identification Techniques



Records & Information Management



Improving Access and Privacy with Records and Information Management

November 2016



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

- Effective records and information management (RIM) practices help institutions **meet legal requirements and better serve the public**
- This paper provides guidance to help institutions understand the relationship between strong RIM practices and compliance with the acts



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

Records & Information Management

Good record management practices:

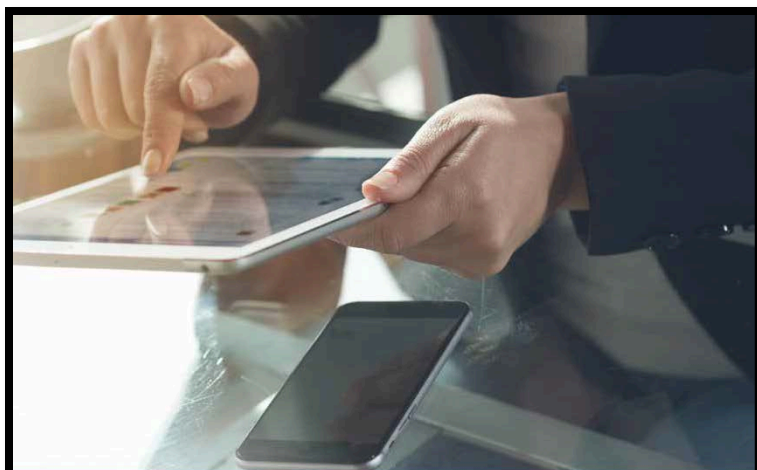
- Improve ability to respond to FOI requests in a timely manner
- **Reduce costs** to organization and requester by making searches more efficient
- Facilitate responses to requests for **correction** of personal information
- **Reduce risk of a privacy breach** and improve privacy breach response
- **Reduce reputational risks** by improving statistical reports and relationships with requesters

Good record management practices also support open government:

- File planning and effective storage ensures that information resources are more easily found and understood, facilitating **proactive disclosure**
- Creation and use of metadata makes data useable and understandable
- Early classification of sensitive records and records containing personal information will help prevent the publication of confidential information
- Retention schedules ensure that records are not inadvertently destroyed



Instant Messaging & Personal Email



Instant Messaging and
Personal Email Accounts:
Meeting Your Access and Privacy
Obligations

June 2016




- Instant messages and emails are considered records under the acts and are subject to FOI requests
- Challenges in managing records produced using personal email or instant messaging:
 - **Search and production** when responding to access to information requests
 - **Retention and preservation** in compliance with the acts
 - Ensuring **privacy and security** of personal information
- We advise institutions to **prohibit use** or enact measures to ensure business records are preserved

New Challenges



Ransomware



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

Technology Fact Sheet

Protecting Against Ransomware

July 2016

Ransomware has become an increasingly common and dangerous threat to the security of electronic records. This fact sheet provides information on how public institutions and healthcare organizations in Ontario can protect themselves against it.

WHAT IS RANSOMWARE?

Ransomware is a type of malicious software, or "malware," that encrypts files on your device or computer, including any mapped or network drives, and then demands payment in exchange for the key needed to decrypt the files. It essentially locks you out of your data and holds the means of regaining access for ransom.

HOW DO COMPUTERS GET INFECTED?

Hackers use different techniques to install ransomware on computers. In general, these fall into two categories: "phishing" attacks and software exploits.

Phishing Attacks

Phishing is a type of online attack in which a hacker sends one or more individuals an unsolicited electronic communication—email, social media post or instant messenger chat—designed to trick or deceive a recipient into revealing sensitive information or downloading malware.

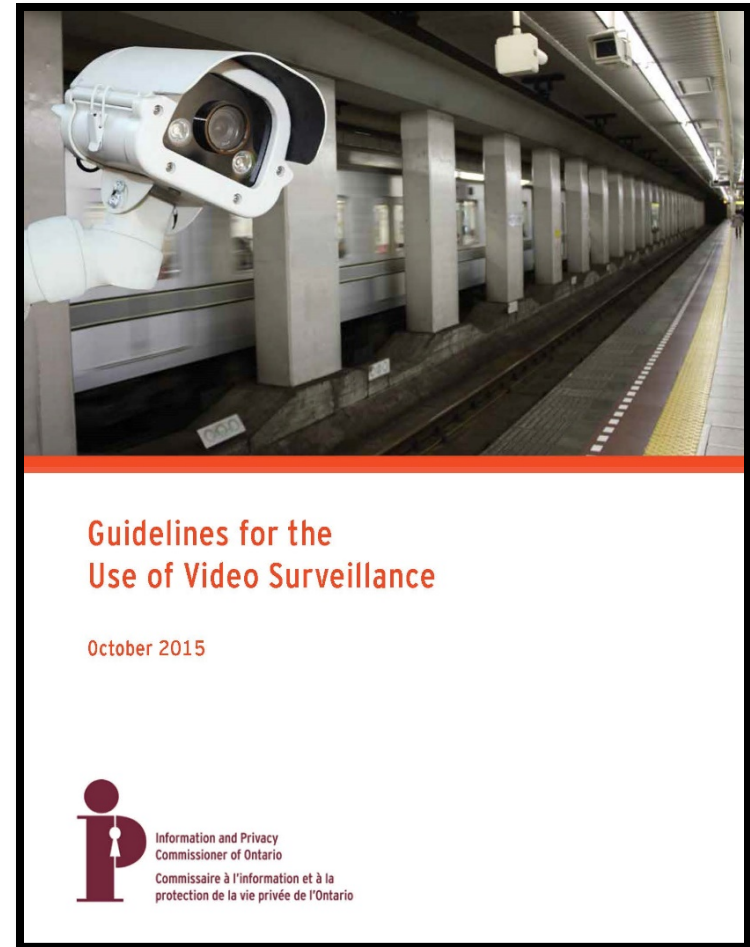
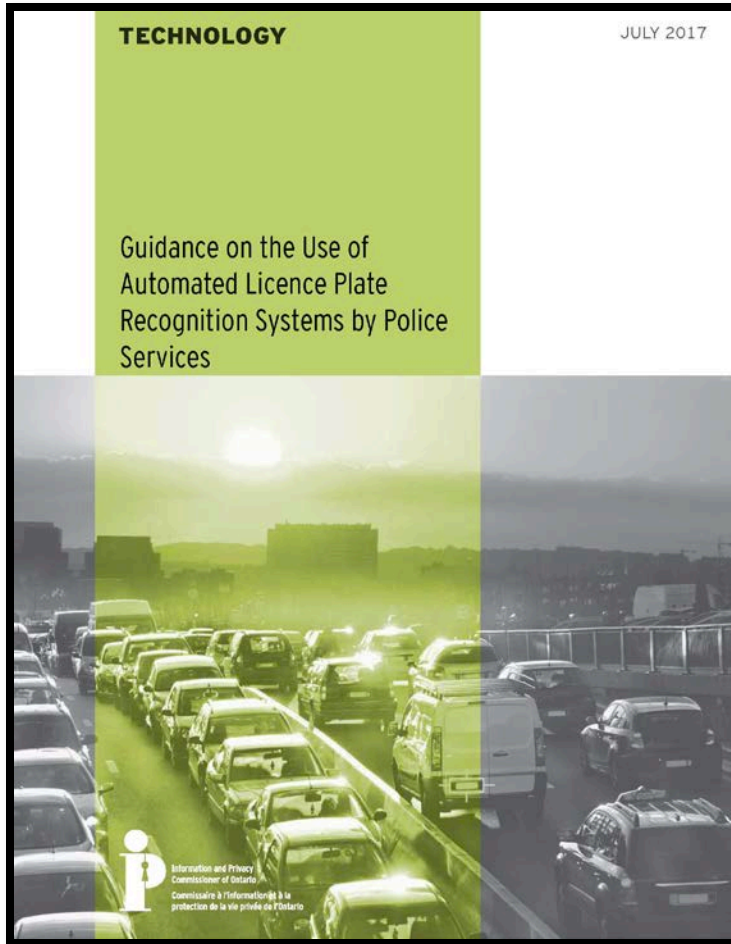
In the case of ransomware, the hacker will often try to impersonate an "official" correspondence relating to a common business transaction, such as a shipping notice or invoice from a delivery company. The hacker may also try to fake an "urgent matter," such as an unpaid invoice or notice of audit. More advanced versions (also known as "spear phishing") target specific individuals or places of business.

Ransomware may be installed if the recipient opens a file attachment or clicks on a link in the body of the message.

- Ransomware is **malicious software** that encrypts files, generally for the purpose of extorting money
- Ways to minimize the risk
 - **only download email attachments or click on links from trusted sources**
 - **avoid opening unsolicited email attachments**
 - **back up all records regularly and check to ensure data is saved**
 - **ensure automatic update of security software, anti-virus programs**



Video Surveillance



Video Surveillance

- Best Practices for municipalities implementing a video surveillance program include:
 - Consulting your **Freedom of Information and Privacy Coordinator** and the public
 - Conducting a **privacy impact assessment (PIA)**
 - Establish **policies** and **procedures**
 - Establish a **privacy breach protocol**
 - **Training** employees
 - **Auditing** roles, responsibilities and practices

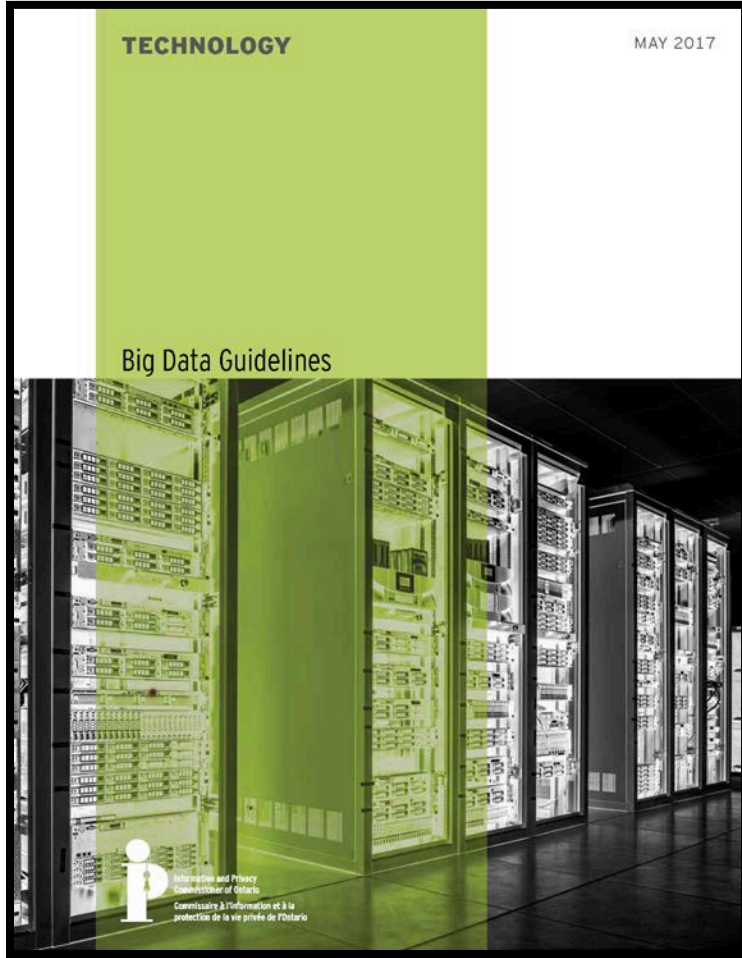


Video Surveillance

- Municipalities should be prepared to process **access requests** from the public including developing protocols for the redaction of personal information from video, where appropriate
- Municipalities may use tools and techniques such as:
 - Digitizing analogue footage to enable the use of more powerful editing tools
 - Blacking out or blurring images of individuals, and
 - Removing the sound of voices
- Retention period of unused images should be limited to the amount of time **reasonably necessary** to discover or report an incident



Big Data



- **Big data generally refers to the use of a number of advancements in computing and technology, including:**
 - new sources and methods of data collection
 - virtually unlimited capacity to store data
 - improved record linkage techniques.
 - algorithms that learn from and make predictions on data
- This paper is designed to inform institutions of key issues and best practices when conducting big data projects involving personal information

Big Data

- *FIPPA/MFIPPA* not designed with big data in mind, as big data-type practices were not possible when the acts were proclaimed (1988/1991):
 - world wide web not yet invented (1989)
 - information technology was less prevalent
 - types of data and analytics were less complex
 - uses of personal information were discrete and determinate.
- May still be possible to conduct big data under *FIPPA/MFIPPA* if collection of personal information (PI) is **expressly authorized by statute** or disclosures are for purpose of **complying with a statute**
 - **Such cases should be the exception, not the rule**
- Institutions should avoid uses of personal information that may be **unexpected, invasive, inaccurate, discriminatory or disrespectful** of individuals



Recent Work on Legislative Reform



Bill 114, Anti-racism Act, 2017

- Bill 114 requires the government to develop and maintain an anti-racism strategy, including targets and indicators
- *Anti-Racism Act (ARA)* would require **prescribed public sector organizations** to collect race-based personal information and use an anti-racism impact assessment framework to promote racial equity in program delivery
- The handling of race-based personal information would be subject to **data standards** and other **privacy requirements**, to be developed in consultation with the IPC



Bill 114, Anti-racism Act, 2017

- Privacy protections include ongoing oversight by our office, notably the authority to:
 - review the collection and use of personal information by public sector organizations, and
 - order an organization to change or discontinue any personal information handling practice that contravenes the *ARA*



Child, Youth and Family Services Act, 2017

- Bill 89 creates a new *Child, Youth and Family Services Act*
- Part X sets out rules for the collection, use and disclosure of **personal information** by child, youth and family service providers (e.g., Minister of Children and Youth Services, Children's Aid Societies)
- Child, youth and family service providers will be subject to **new privacy and access rules** overseen by the IPC
- Includes **broad powers to share personal information** between government organizations
- This Act is not yet in force



Child, Youth and Family Services Act, 2017

- March 2017, IPC submission to the Standing Committee focused on significant privacy issues:
 - the ministry must be subject to a greater degree of **accountability and oversight** than what is currently provided
 - the bill should be amended to strengthen **privacy safeguards** and to narrow the ministry's powers to collect, use and disclose personal information to what is reasonably necessary
 - the authority to **share personal information** among government organizations and to disclose it to persons and entities that are not prescribed in the regulations must be removed from the legislation



Questions?



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

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



Information and Privacy
Commissioner of Ontario

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