

REACHING OUT
TO ONTARIO

Latest Developments in Access and Privacy

Brian Beamish
Information and Privacy Commissioner of Ontario

Sherry Liang
Assistant Commissioner

Barrie

November 23, 2018



REACHING OUT TO ONTARIO

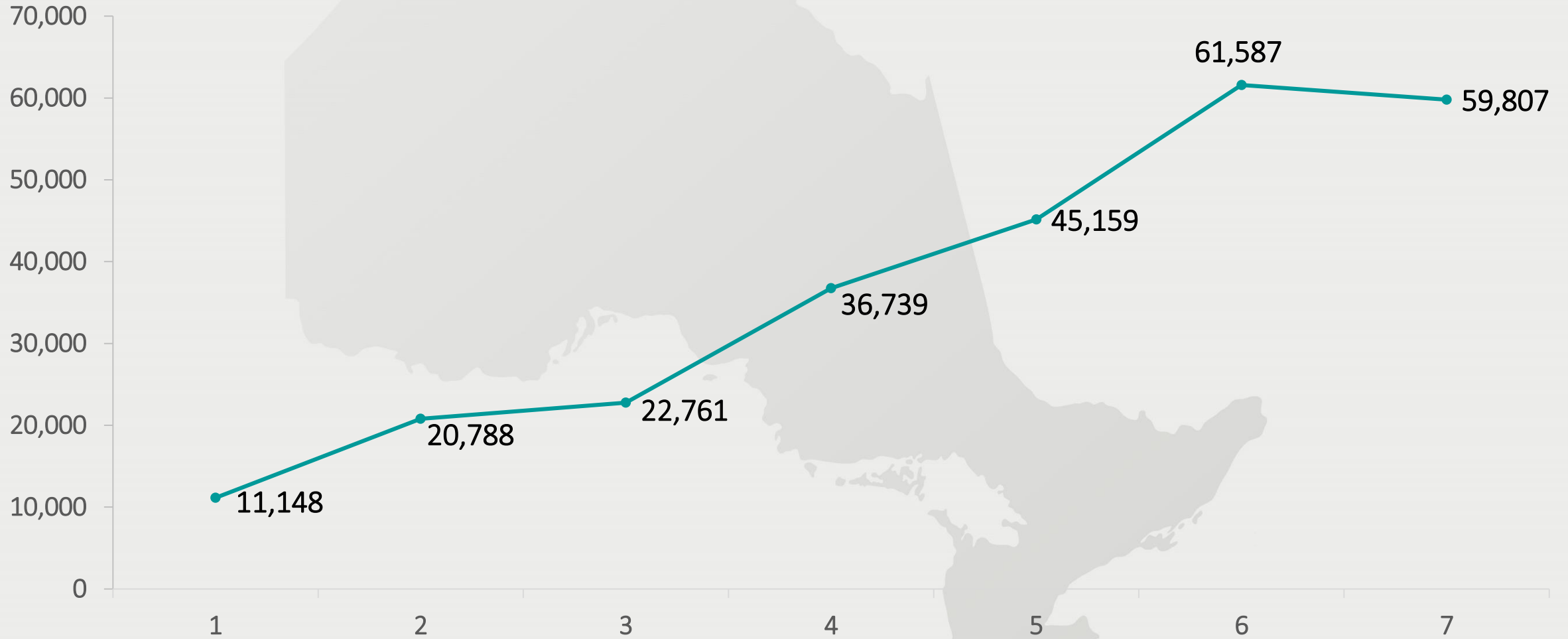
ROTO is an ongoing program where we visit communities across Ontario and host events to discuss the latest developments in access and privacy with stakeholders and the public



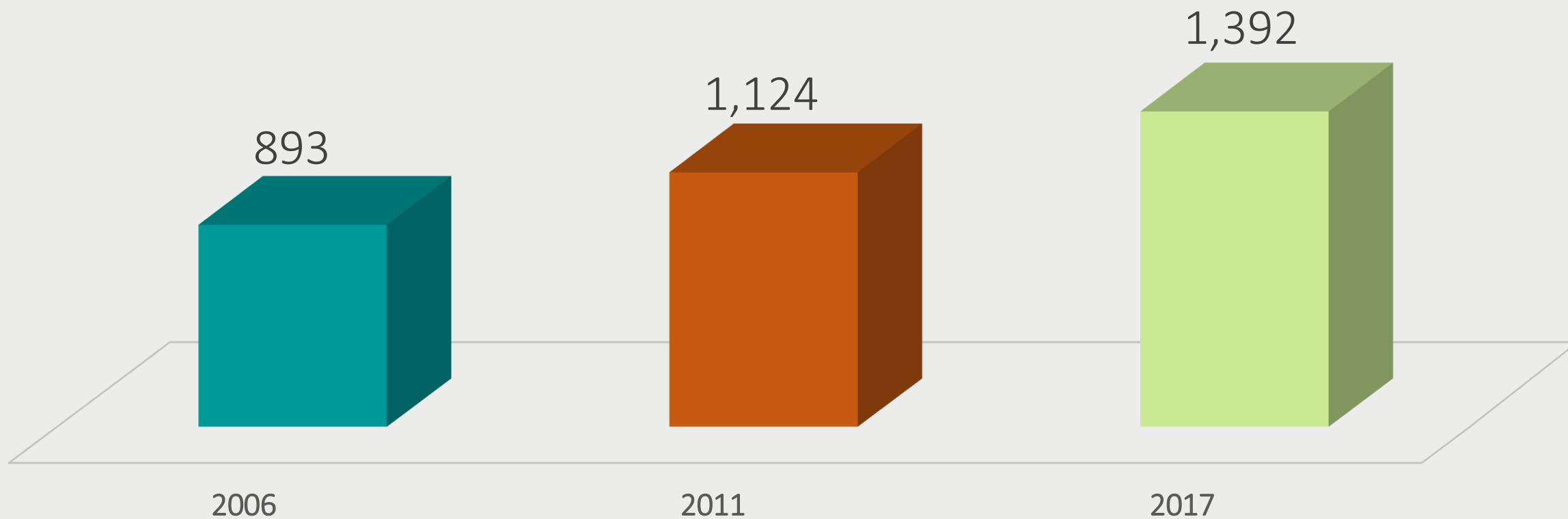
- St. Catharines
- Ottawa
- Sault Ste. Marie
- Kingston
- Barrie
- London
- Thunder Bay
- Windsor
- Hamilton

REACHING OUT
TO ONTARIO

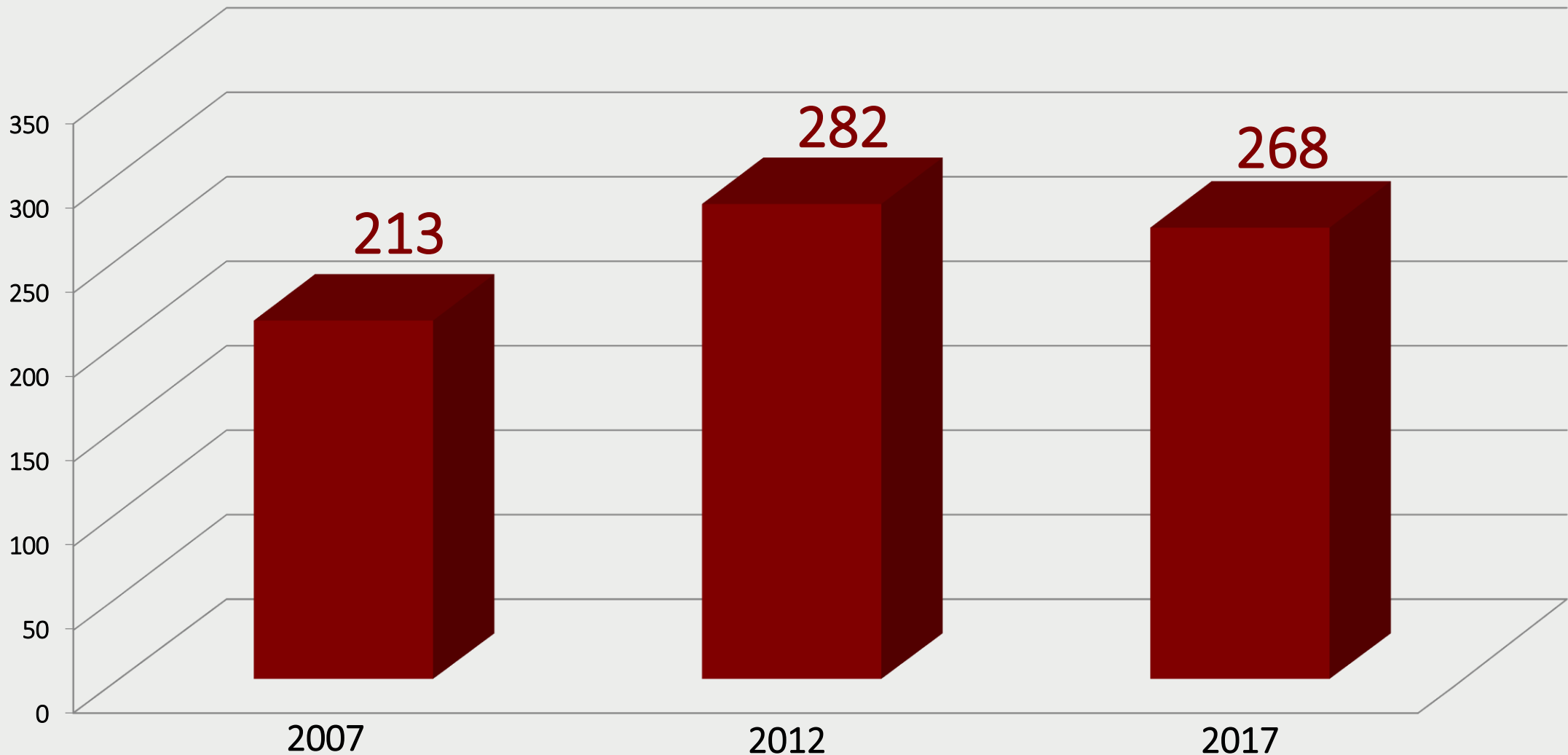
Access Requests Per Year



Appeals Received per Year



Total Privacy Complaints Opened Per Year



Mediation: Critical to Our Success

- Usually, 75 per cent of appeals and almost all privacy complaints are closed before adjudication/investigation
- Goal is to find a resolution which satisfies the needs of all involved
- Saves significant time and resources for all parties

Smart Cities

- A community that uses connected technologies to collect and analyze data to improve services for citizens
 - energy conservation sensors that dim streetlights when not in use
 - parking apps that indicate nearest available public parking spot
 - garbage cans that send a signal when full



Privacy Risks of Smart Cities

- Information may be collected by municipalities, contractors, or private sector companies
- Must ensure collection, use and disclosure is authorized
- Information must be safeguarded from cyberattack
- Must ensure smart cities do not become infrastructures for mass surveillance



Minimize Privacy Risks

- Strong safeguards can protect personal information
 - privacy impact and threat/risk assessments
 - data minimization
 - de-identified data
 - encryption
 - privacy and access governance
 - contracts with private sector partners that address ownership of data
 - community engagement and project transparency
- IPC is working with municipalities and federal government
 - encourage transparency
 - ensure that privacy protections are built into smart city initiatives



- Developed to help the public understand smart cities and the impact they can have on personal privacy



Data Analytics

- Change how we think about and use data
- New combinations of data may reveal hidden patterns and insights
- Data integration (sharing, linking, analyzing data) can enhance
 - policy development
 - system planning
 - resource allocation
 - performance monitoring



Privacy Risks of Data Integration

- not based on consent – lack of transparency
- Creation of multiple massive government databases of personal information
- surveillance and profiling of individuals
- increased cybersecurity risks
- potential discrimination based on inaccurate data/flawed algorithms

The Need for Legislative Reform

- *FIPPA* treats government institutions as silos; indirect collection, sharing/linking across government not envisioned
- Call for single dedicated unit in Ontario to:
 - collect PI across government
 - link records securely
 - de-identify
 - make de-identified data available to public bodies
- Would mirror *PHIPA* approach [s. 55.9]
- Avoids multiple databases, profiles of sensitive PI across government

Surveillance Technologies

- IPC supports use of surveillance technologies to enhance community safety and deter unlawful activity, providing they are implemented in a manner that protects privacy
- Privacy implications associated with surveillance technologies include:
 - Potential to collect large amounts of personal information about individual users, including who they communicate with and what they communicate about
 - Ability to track the locations of individuals over time and to facilitate profiling of law-abiding individuals going about their everyday activities

Sudbury's "Eye in the Sky"

- For many years, the Sudbury Police have operated the "Lions' Eye in the Sky" program, using cameras on downtown streets live-monitored by volunteers
- A recent expansion of the program led the IPC to review the program to ensure it complied with privacy law
- IPC decided the program and the expansion were justified
- Our policy department worked with the police to make sure the details of the surveillance complied with privacy best practices

Body-Worn Cameras

- Continuous recording collects more information than necessary for the law enforcement purpose
- Microphones capture ambient sound, including the conversations of bystanders
- Used inside private homes, increases the likelihood individuals will be recorded in highly personal situations



City of Hamilton CCTV and Private Properties



VIA ELECTRONIC MAIL

February 13, 2018

Fred Eisenberger
Mayor
City of Hamilton
Hamilton City Hall
2nd Floor, 71 Main Street West
Hamilton, ON L8P 4Y5

Eric Girt
Police Chief
Hamilton Police Service
155 King William Street
Box 1060, LCD1
Hamilton, ON L8N 4C1

Dear Mayor Eisenberger and Chief Girt:

Re: CCTV cameras and private properties

I am writing to you about a significant privacy issue involving the City of Hamilton's proposed use of CCTV images taken by private individuals. Council's General Issues Committee passed a motion on February 7, 2018, that city staff work with the Hamilton Police Service to review the current CCTV by-law applicable to private homes and assess the feasibility of amending it to permit the collection of personal information from public spaces for use by the police.

As you know, my office oversees the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*, which applies to municipal government institutions and law enforcement agencies, and sets rules for protecting the privacy rights of Ontarians. The use of surveillance cameras by the city or police, and the collection of images from private cameras, must comply with this law.

In my view, any attempt by the city to permit or encourage the use of private video surveillance cameras, for the purpose of collecting personal information to aid in law enforcement, would undermine privacy rights under *MFIPPA*.

While in some cases CCTV surveillance may enhance public safety and the security of assets, it also poses risks to the privacy of individuals whose personal information may be collected, used and disclosed. The risk to privacy is particularly acute because video surveillance may, and often does, capture the personal information of law-abiding individuals going about their everyday activities. In view of the broad scope of personal information collected, special care must be



Tel: (416) 326-3333
1 (800) 387-0073
Fax/Télé: (416) 325-9195
TTY: (416) 325-7539
Web: www.ipc.on.ca

- Hamilton is reviewing CCTV by-law to assess feasibility of amendment to permit police to collect footage from security cameras of citizens
- Coverage is currently restricted to owner's property, amended by-law would enable broader coverage
- Hamilton is encouraged to leave the by-law un-amended



REACHING OUT TO ONTARIO

- Hackers infected the town's servers with a code that locked staff out of files and data, including the personal tax information of residents
- Town paid the ransom to regain access to its servers
- Town has since installed a secure offsite backup that will protect the municipality's computer data

Ransomware Attacks

MONDAY, JUNE 4, 2018
12 °C

Simcoe.com SUBMIT YOUR CONTENT | SIGN IN
metrolandmedia
Connected to your community

FULL MENU LOCAL NEWS WHAT'S ON COMMUNITY CRIME EVENTS EXPLORE SIMCOE CLASSIFIEDS OBITUARIES SEARCH


Home / News / Council / **How Wasaga Beach Plans To Keep Its Data...**

How Wasaga Beach plans to keep its data secure in wake of recent ransomware attack

A few weeks ago, hackers were able to infect municipal servers

NEWS May 26, 2018 by Chris Simon Wasaga Sun

f t r in e



Wasaga Beach town hall - Metroland file photo

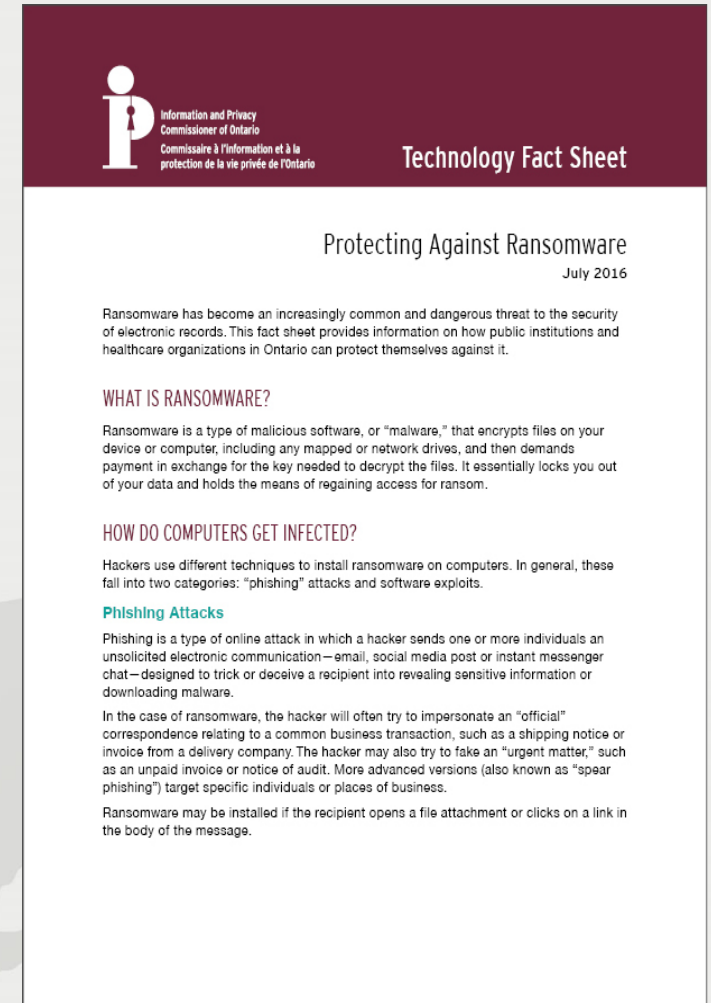
TOP STORIES

NEWS Jun 03, 2018
Coast Guard rescues two people after boat sinks in Georgian Bay

PROVINCIAL ELECTION Jun 03, 2018
Voter who tried to decline ballot met with 'blank faces' at Barrie advanced...

Protecting Against Ransomware

- 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 and anti-virus programs
- Security software should receive automatic notices and perform real-time scans



REACHING OUT
TO ONTARIO

LEGISLATION



Child, Youth and Family Services Act

- The *CYFSA* received Royal Assent on June 1, 2017
- Part X of the *CYFSA* was proclaimed along with the rest of the *CYFSA* on April 30, 2018, but will come into effect on January 1, 2020
- Part X of the *CYFSA* represents a big step forward for Ontario's child and youth sectors:
 - closes a legislative gap for access and privacy
 - promotes transparency and accountability

Child, Youth and Family Services Act

- Strengths of Part X:
 - modelled after *PHIPA*
 - consent-based framework
 - individuals' right of access to their personal information
 - mandatory privacy breach reporting
 - clear offence provisions
 - adequate powers for the IPC to conduct reviews of complaints
 - facilitates transparency and consistency among CASs' information practices

Child, Youth and Family Services Act

- Part X gives individuals the right to access:
 - records of their personal information (PI)
 - in a service provider's custody or control and
 - that relate to the provision of a service to the individual
- No fees can be charged for access except in prescribed circumstances (currently, none are prescribed)
- Appeal access decisions to IPC

Police Record Checks Reform Act

- Became law on November 1, 2018
- Reflects over a decade of input from our office
- Changes the rules about what police can tell prospective employers, volunteer agencies and foreign governments about Ontarians
- Protects individuals from the release of unproven allegations and mental health records in police background checks
- First law of its kind in Canada



REACHING OUT
TO ONTARIO

GUIDANCE



Fees, Fee Estimates and Fee Waivers

- A number of important orders and court decisions have been issued since the original guide was first published in 2003.
- This updated version explains:
 - factors to consider when calculating fee
 - how to provide a reasonable fee estimate and interim decision
 - how interim access decisions affect timelines
 - what decisions may be appealed
 - how a fee waiver is determined

ACCESS

JUNE 2018

Fees, Fee Estimates and Fee
Waivers



Lesson Plans for Educators: Privacy Rights, Digital Literacy and Online Safety

LESSON PLAN

Level: Grades 6 to 8
Duration: 2 to 4 hours—Approximately two hours lesson time; work time for the assessment/evaluation task will vary.

This lesson was created by MediaSmarts for Canada's federal, provincial and territorial privacy protection authorities.

Getting the Toothpaste Back into the Tube: A Lesson on Online Information

Overview

In this lesson, students watch a short video that compares getting rid of personal information online to getting toothpaste back into a tube. After a short discussion of how visual analogies like this work, students discuss the meaning of the video (that information online is *permanent*). They then read a series of short scenarios that help them identify four further principles of information online: that it can be *copied*, that it can be seen by *unintended audiences*, that it can be seen by *larger audiences* than intended, and that it becomes *searchable*. Finally, students create a simple animation that illustrates one of these principles.

Learning Outcomes

Students will:

- Learn key principles relating to online privacy in the context of digital literacy and related subject areas, in particular that online information:
 - is permanent;
 - can be copied;
 - can be seen by unintended, and potentially much larger audiences;
 - and is searchable.
- Understand visual analogies in the context of language arts and related subject areas
- Create a media product in the context of language arts and/or media literacy and related subject areas

This lesson plan also addresses the development of several key privacy education competencies in the [Personal Data Protection Competency Framework for School Students](#), including:

- Understanding the concept of personal information;
- Understanding the digital environment – technical aspects;
- Understanding personal information regulations – controlling the use of personal information



1

LESSON PLAN

Level: Grades 6 to 8
Duration: 60-90 minutes class time, plus time in class or at home to complete the evaluation task

This lesson was created by MediaSmarts for Canada's federal, provincial and territorial privacy protection authorities.

Know the Deal: The Value of Privacy

Overview

In this lesson, students are introduced to the idea that privacy is a fundamental human right and that their personal information is valuable. The lesson focuses on the "economics" of personal information and that most "free" apps and online services make some or all of their revenue by collecting (and in some cases reselling) users' personal information. Students will watch a video that illustrates the idea that they may be paying with their privacy and then discuss some of the ramifications of this. They will learn about tools and techniques for minimizing the personal information they share and create a public service announcement that helps them and their peers "know the deal" about the value of privacy.

Learning Outcomes

Personal information:

Students will understand:

- the concept of personal information
- the concept of pseudonymity and masking one's identity
- that privacy is valuable and a fundamental human right and it means you have a choice of what personal information to share and with whom
- that online activity may leave traces which can contain personal information

Students will develop the ability to:

- recognize types of personal information that can be used to directly identify individuals, and information that can be used to monitor and identify a person online

Understanding the digital environment:

Students will understand:

- the concept of information architecture, and the collection, structure, and processing of information
- how to recognize key players in the digital economy



LESSON PLAN

Level: Grades 9 to 12
Duration: 1.5 — 2 hours

This lesson was created by MediaSmarts for Canada's federal, provincial and territorial privacy protection authorities.

Privacy Rights of Children and Teens

Overview

In this lesson, students are introduced to the privacy principles that inform the Alberta and BC *Personal Information Protection Acts*, Québec's *An Act Respecting the Protection of Personal Information in the Private Sector* and the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) relating to personal information collection online. They learn ways to find out what personal information may or has been collected by platforms that they use, how to limit data collection about themselves, and the various forms of recourse that are available to them if they feel an organization is not respecting their rights.

Learning Outcomes

Students will learn:

- that they have legal and consumer rights with regards to personal information
- to evaluate how well the online platforms and services they use live up to those rights
- which federal, provincial and territorial laws and offices oversee privacy concerns
- how to make a privacy complaint
- how to create a media product in the context of language arts and/or media literacy and related subject areas

Preparation and Materials

- Arrange access to a computer lab or ensure that at least seven students have devices able to access the Internet (preferably laptops or tablets, as students will be reviewing Terms of Service and Privacy Policies)
- Photocopy the following handouts:
 - [Privacy Protection Principles](#)
 - [Protecting Your Privacy](#)
 - [Fair Information Principle Group Activity](#); Close Reading Table
- Photocopy the assignment sheet [Your Privacy, Your Rights](#)



1

Europe's General Data Protection Regulation (GDPR)

- Came into effect on May 25, 2018
- Applies to the collection, use and disclosure of personal data by organizations inside the EU
- However, it may apply to organizations based in Ontario if they:
 - offer goods and services to individuals in the EU
 - monitor the behaviour of individuals in the EU
- How the law is applied and interpreted will depend on the EU data protection authorities and courts

General Data Protection Regulation

OVERVIEW

The European Union's (EU) General Data Protection Regulation (GDPR) is a privacy law that came into force on May 25, 2018. It is designed to give individuals in the EU control over how their data are processed and used.

Although it is an EU law, the GDPR may apply to public institutions and health information custodians in Ontario in certain limited circumstances. The Information and Privacy Commissioner of Ontario (IPC) does not oversee or enforce the GDPR.

This fact sheet provides institutions and custodians in Ontario with general information about the potential application of this law, and some of its key requirements. Some GDPR requirements may go beyond the privacy rules set out in the *Freedom of Information and Protection of Privacy Act (FIPPA)*, the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*, and the *Personal Health Information Protection Act (PHIPA)*.

This fact sheet is not a legal interpretation of any provision of the GDPR and does not provide legal advice about its application in Ontario. Organizations should consult their legal counsel for advice. The scope of the law's application and the interpretation of its requirements depend on future decisions and guidance issued by the EU data protection authorities and courts.

Access Fact Sheet: Third Party Information Exemption

- An institution must first determine if the third party exemption applies before withholding records.
- Three-part test:
 - the record contains certain types of business information
 - the information was supplied in confidence, either implicitly or explicitly
 - disclosure could cause harm to the third party

Third Party Information Exemption

Public institutions typically have information about outside, or “third party” organizations. Often this information is collected from organizations doing business with institutions. While Ontario’s *Freedom of Information and Protection of Privacy Act* and *Municipal Freedom of Information and Protection of Privacy Act* give people the right to access records held by institutions, there are exceptions to that right, including where disclosure could harm a third party’s business interests. This exception is commonly referred to as the “third party exemption.”

When an institution receives a request for records that include information related to a third party, it must determine if the third party exemption applies to justify withholding the records.

DETERMINING IF THE EXEMPTION APPLIES

The exemption applies if the record satisfies all three parts of this test:

1. the record contains certain types of business information
2. the information was supplied in confidence, either implicitly or explicitly
3. disclosure could cause harm to the third party

Privacy Fact Sheet: Disclosure of Personal Information to Law Enforcement

- When can institutions disclose personal information to a law enforcement agency?
 - when legally required
 - to aid a law enforcement investigation
 - for health or safety reasons
- Disclosing institutions need to:
 - document disclosure requests and court orders
 - be transparent about their decisions
 - develop and publish policies about how they make and document decisions about disclosure

Disclosure of Personal Information to Law Enforcement

Under Ontario's access and privacy laws, institutions are prohibited from disclosing personal information, except in defined situations.

This fact sheet describes the key situations where institutions (public sector organizations such as provincial ministries and agencies, municipalities, schools, transit systems) can disclose personal information to a law enforcement agency under the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act*. It also explains how to respond when a law enforcement agency requests personal information, and how to be transparent to the public about disclosure decisions.

Generally, institutions should disclose personal information to a law enforcement agency *only when required by law*, such as in response to a court order, rather than a simple request, where there is no requirement to disclose.

However, they have the discretion to disclose in other situations, including where disclosure is made to aid an investigation, and for health or safety reasons.

In all cases, an institution should make its own careful and informed assessment of the circumstances before deciding whether to disclose personal information to a law enforcement agency. If uncertain, it should seek legal advice.

REACHING OUT
TO ONTARIO

RECENT DECISIONS



Personal Email Accounts of Elected Officials

- **Order MO-3607** – Township of Springwater received a request for all emails from the non-township email accounts of the Mayor, Deputy Mayor and a councillor, related to land development within the township
- Township denied access citing that it did not have custody or control of the records
- IPC received submissions from Mayor, Deputy Mayor and councillor
- No evidence that they used personal email accounts to conduct township business
- Any emails to conduct township business are available on township email accounts
- Emails in personal email accounts are not in custody or control of township

Can Councillors' Records Be Accessed Through *MFIPPA*?

- **Order MO-3471** – request for access to communications sent or received by staff relating to city councillor's Twitter account
- IPC rules records are personal/political, relating to councillor's activities as an elected representative
- Therefore, not accessible (outside city's custody or control)



Sale of Taxi Cab Licenses

- **Order MO-3673** – City of Hamilton received request for specific taxi-cab license sale prices, the sale dates, and license numbers associated with those sales.
- City denied access, citing third party and personal privacy exemptions
- Decision: Information about sale of taxi cab licenses is not personal
- Information also not covered by exemption for third party business information

Compelling Public Interest: Police Carding

- **Order MO-3476** – requester seeks information about street checks and racial data from Peel police
- Police deny access to six records, claiming they contain advice and recommendations
- IPC agrees that they contained advice and recommendations
- However, applies public interest override in MFIPPA (section 16)
- For most of the records, a compelling public interest in disclosure outweighs the purpose of not revealing advice and recommendations
- Order to police to disclose 5 of 6 records

Pursuing Remedy for Dog Bites

- **Order MO-3370** – individual requests name and address of owner of dog that bit them
- City of Hamilton grants access to records documenting the incident, but withholds dog owner’s personal information
- Individual appeals, claiming identity and address necessary to continue their dog bite liability case
- IPC orders release of name and address; non-disclosure restricted individual’s right to pursue legal action

Frivolous and Vexatious Requests

- **Order PO-3691** – 40 requests in nine weeks to Public Guardian and Trustee (PGT) related to a deceased person's estate
- PGT limits number of requests the requester can make at one time
- Requester appeals
- IPC views high volume of requests as interfering with the operations of the institution
- Finds requests “frivolous and vexatious”

REACHING OUT
TO ONTARIO

PRIVACY COMPLAINTS



School Photos

- **Privacy Complaint MC16-5** – complaint by a parent about school photos
- **Conclusions/Findings:**
 - collection and use of students' photographs for education-related purposes is permissible
 - however, use of photos for ID cards in association with Canadian Centre for Child Protection goes beyond original purpose
- **Recommendations:**
 - That Parents/guardians:
 - be provided with the opportunity to opt out of receiving marketing from photographers
 - be provided with the opportunity to opt out of the identification card program
 - be able to request the photographer destroy their children's personal information so long as it does not interfere with the Board's administrative requirements

Tribunal Decisions

- **Privacy Complaint PC17-9** – complaint made about personal information in a published decision of the Human Rights Tribunal of Ontario's (HRTO)
- **Conclusions/Findings:**
 - HRTO's publication of personal information does not come under FIPPA
 - HRTO's decisions are not covered by the privacy rules in FIPPA because information is in those decisions for the purpose of creating a public record
- **Recommendation:**
 - HRTO only include minimum personal information necessary to the purpose of the decisions

REACHING OUT
TO ONTARIO

MEDIATION SUCCESS STORIES



Toronto Transit Commission

- Toronto Transit Commission (TTC) received an access request for all communications, emails, briefing notes, draft and internal reports relating to the Scarborough subway/LRT, for periods from 2010 to 2017
- TTC issued a fee estimate of \$31,948.50 and a time extension of one to three years
- Through mediation and discussions including knowledgeable city staff, the appellant narrowed the scope of the request over time, city gave reduced fee estimates, and the fee estimate was eventually reduced to \$707.00

Ministry of the Environment and Climate Change

- A citizen's group, made an access request to the Ministry of the Environment and Climate Change for records relating to concerns about wells near a quarry
- After notifying an affected third party, the ministry granted partial access to the records but denied access to others based partly on personal privacy
- The third party (owner of the quarry) also filed an appeal objecting to the ministry's decision to grant partial access
- Through mediation, the third party consented to disclose all of the records at issue and also invited the citizen's group to view the quarry site and ask questions

REACHING OUT
TO ONTARIO

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

