Recent Developments at the IPC

Brian Beamish

Information and Privacy Commissioner
of Ontario

Information and Privacy
Commissioner of Ontario

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

AMCTO Municipal
Information Access
and Privacy Forum

November 30, 2018

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

- Privacy is not a barrier to smart cities, but they require robust privacy protections
- Without safeguards in place, large amounts of personal information may be collected, used, disclosed
- Potential hazards:
  - tracking individuals as they go about their daily activities (surveillance)
  - using information for other purposes without consent (scope creep)
  - security breaches (cyberattacks)

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

Fact Sheet

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

APRIL 2018

TECHNOLOGY FACT SHEET

Smart Cities and Your Privacy Rights

New technologies promise to help municipalities better manage urban environments and deliver services in a more effective and efficient way. They can help to make communities more liveable, sustainable, and fair. Many involve the collection and use of large amounts of information, including personal information. Cities or municipalities that use these connected technologies are often described as "smart cities."

This fact sheet was developed to help members of the public understand smart cities and how they can impact an individual's privacy

The Office of the Information and Privacy Commissioner of Ontario (IPC) provides independent oversight of the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*). This act protects the privacy of personal information by setting rules for its collection, use and disclosure by municipalities and municipal institutions. These rules also give individuals the right to access their own personal information.

The IPC has developed this fact sheet to help the public understand smart cities and how they can impact an individual's privacy.

WHAT ARE "SMART" CITIES?

Smart cities use technologies that collect data to improve the management and delivery of municipal services, support planning and analysis, and promote innovation within the community. By collecting large amounts of data, often in real-time, municipalities can gain a greater understanding of the quality and effectiveness of their services. For example, commuter traffic flow data can identify congestion

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

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

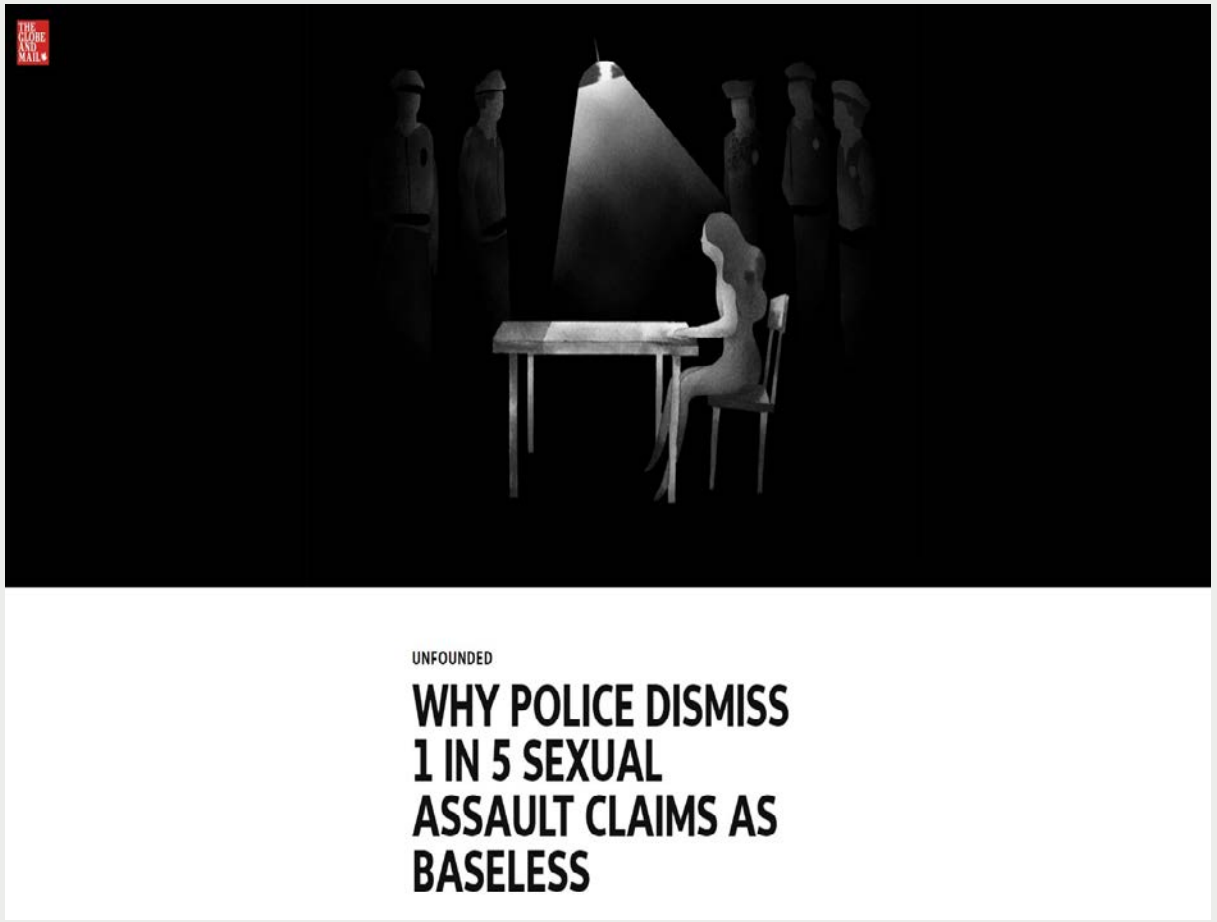
- *FIPPA* treats government institutions as silos; indirect collection, sharing/linking across government not envisioned
- Call for single dedicated unit in Ontario to:
  - collect PI across government
  - link records securely
  - de-identify
  - make de-identified data available to public bodies
-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

Making Political Parties Subject to Privacy Laws

- Political parties are not covered by privacy laws (except BC)
- Digital tools can amass large amounts of personal information, analyze it and target people in granular and unique ways
- Increasingly sophisticated data practices raise new privacy and ethical concerns
- Data is vulnerable to cybersecurity threats
- IPC annual report recommendation – Ontario's political parties should be subject to privacy regulation and oversight
- Recent resolution of Fed/Prov/Terr Privacy Commissioners

The Philadelphia Model

- Review of police sexual assault files to look for deficiencies and biases
- Since implementation in Philadelphia 17 years ago, “unfounded rape” rate dropped to four per cent
- U.S. national average is seven per cent



Globe and Mail Series:
Unfounded
Robyn Doolittle

Ontario-based Philadelphia Model

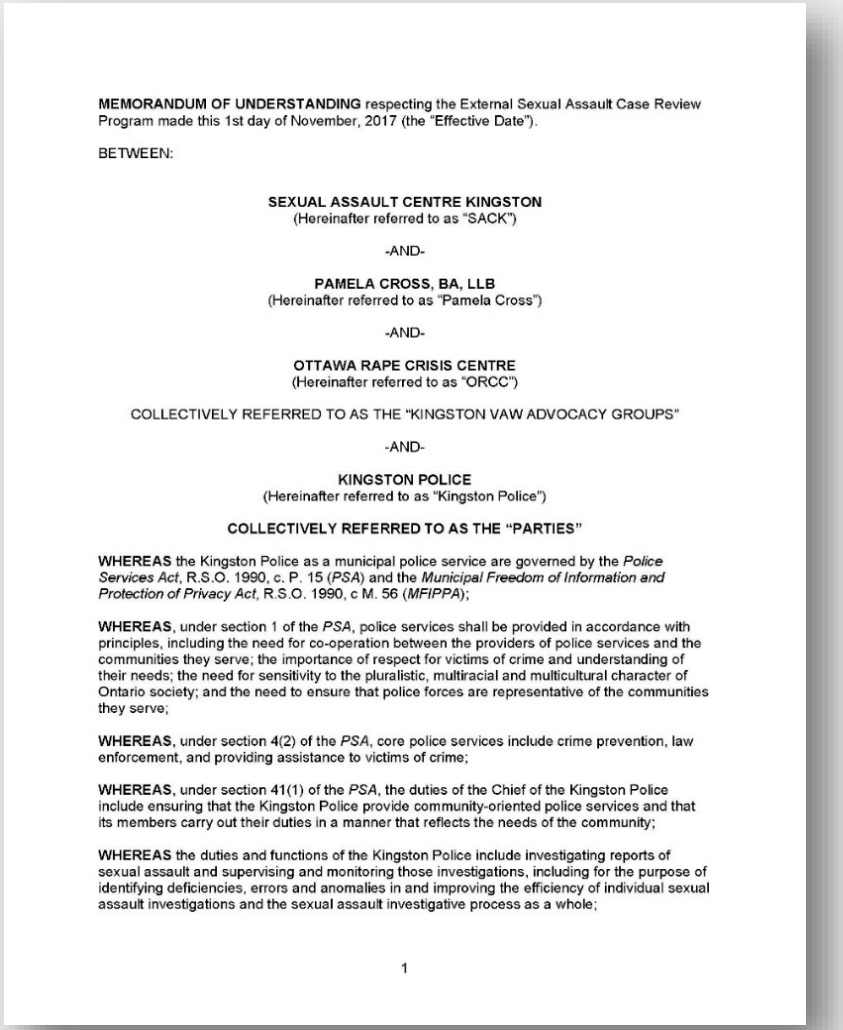
Cont'd

- Identify external partners with experience to assist in review and appoint them 'agents of the service'
- Ensure external reviewers have background check, sign an oath of confidentiality and receive privacy and confidentiality training
- Require external reviewers to see names of principals so they can recuse themselves if needed
- Permit external reviewers to review complete closed files, subject only to redactions or restrictions required by law
- Ensure reviews take place at police facilities and no identifying information is copied, retained, or removed by agents

MOU for Use by Ontario Police

Cont'd

- IPC worked with police and stakeholders to develop model Memorandum of Understanding and Confidentiality Agreement
- Sets the terms for review of sexual assault cases by police and external reviewers
- Kingston Police are first to put into practice



MEMORANDUM OF UNDERSTANDING respecting the External Sexual Assault Case Review Program made this 1st day of November, 2017 (the "Effective Date").

BETWEEN:

SEXUAL ASSAULT CENTRE KINGSTON
(Hereinafter referred to as "SACK")

-AND-

PAMELA CROSS, BA, LLB
(Hereinafter referred to as "Pamela Cross")

-AND-

OTTAWA RAPE CRISIS CENTRE
(Hereinafter referred to as "ORCC")

COLLECTIVELY REFERRED TO AS THE "KINGSTON VAW ADVOCACY GROUPS"

-AND-

KINGSTON POLICE
(Hereinafter referred to as "Kingston Police")

COLLECTIVELY REFERRED TO AS THE "PARTIES"

WHEREAS the Kingston Police as a municipal police service are governed by the *Police Services Act*, R.S.O. 1990, c. P. 15 (*PSA*) and the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c M. 56 (*MFIPPA*);

WHEREAS, under section 1 of the *PSA*, police services shall be provided in accordance with principles, including the need for co-operation between the providers of police services and the communities they serve; the importance of respect for victims of crime and understanding of their needs; the need for sensitivity to the pluralistic, multiracial and multicultural character of Ontario society; and the need to ensure that police forces are representative of the communities they serve;

WHEREAS, under section 4(2) of the *PSA*, core police services include crime prevention, law enforcement, and providing assistance to victims of crime;

WHEREAS, under section 41(1) of the *PSA*, the duties of the Chief of the Kingston Police include ensuring that the Kingston Police provide community-oriented police services and that its members carry out their duties in a manner that reflects the needs of the community;

WHEREAS the duties and functions of the Kingston Police include investigating reports of sexual assault and supervising and monitoring those investigations, including for the purpose of identifying deficiencies, errors and anomalies in and improving the efficiency of individual sexual assault investigations and the sexual assault investigative process as a whole;

1

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"

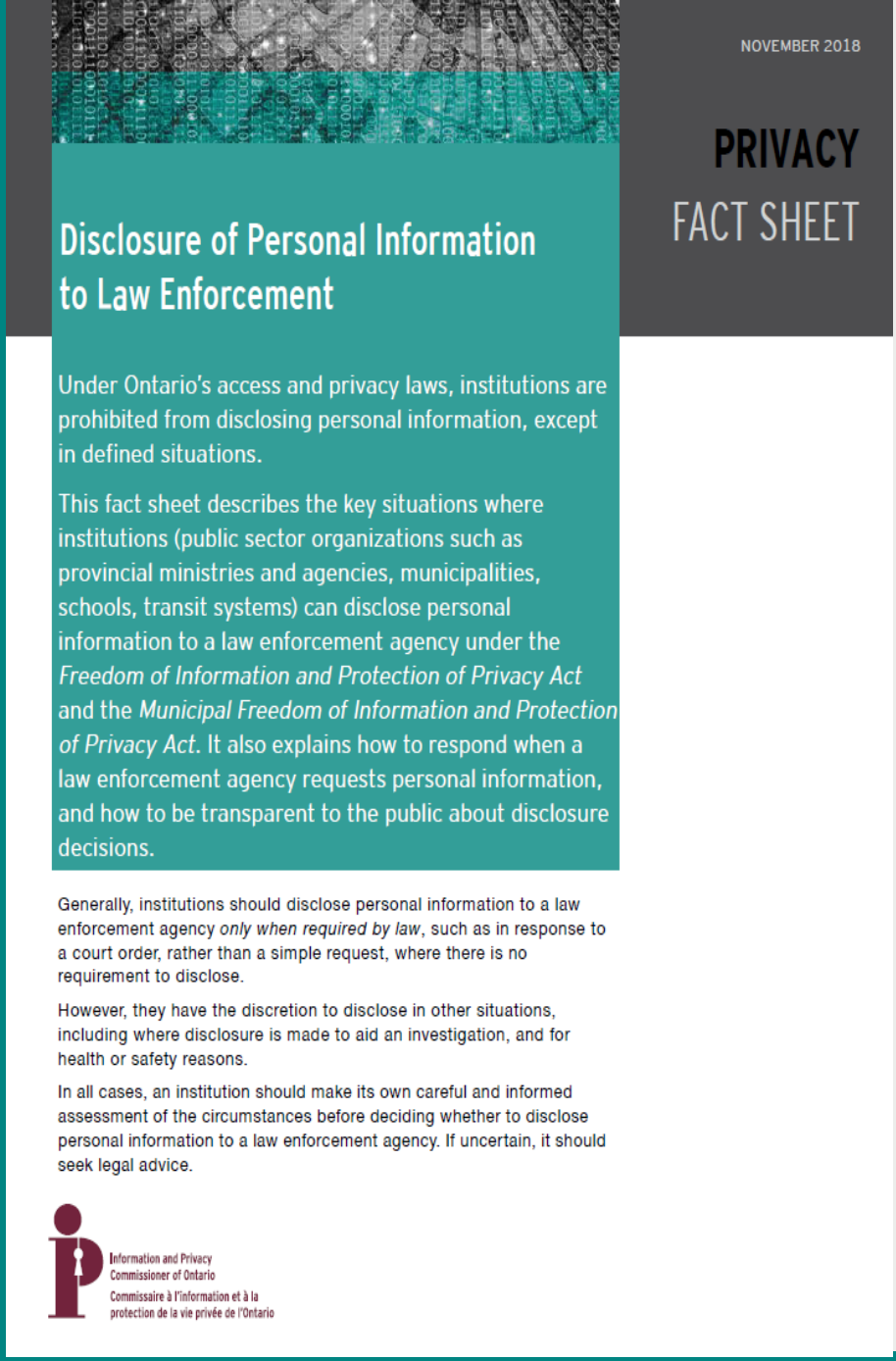
- For many years, the Sudbury Police have operated the "Lions' Eye in the Sky" program, using cameras on downtown streets live-monitored by volunteers
- A recent expansion of the program led the IPC to review the program to ensure it complied with privacy law
- IPC decided the program and the expansion 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

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



NOVEMBER 2018

PRIVACY
FACT SHEET

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.

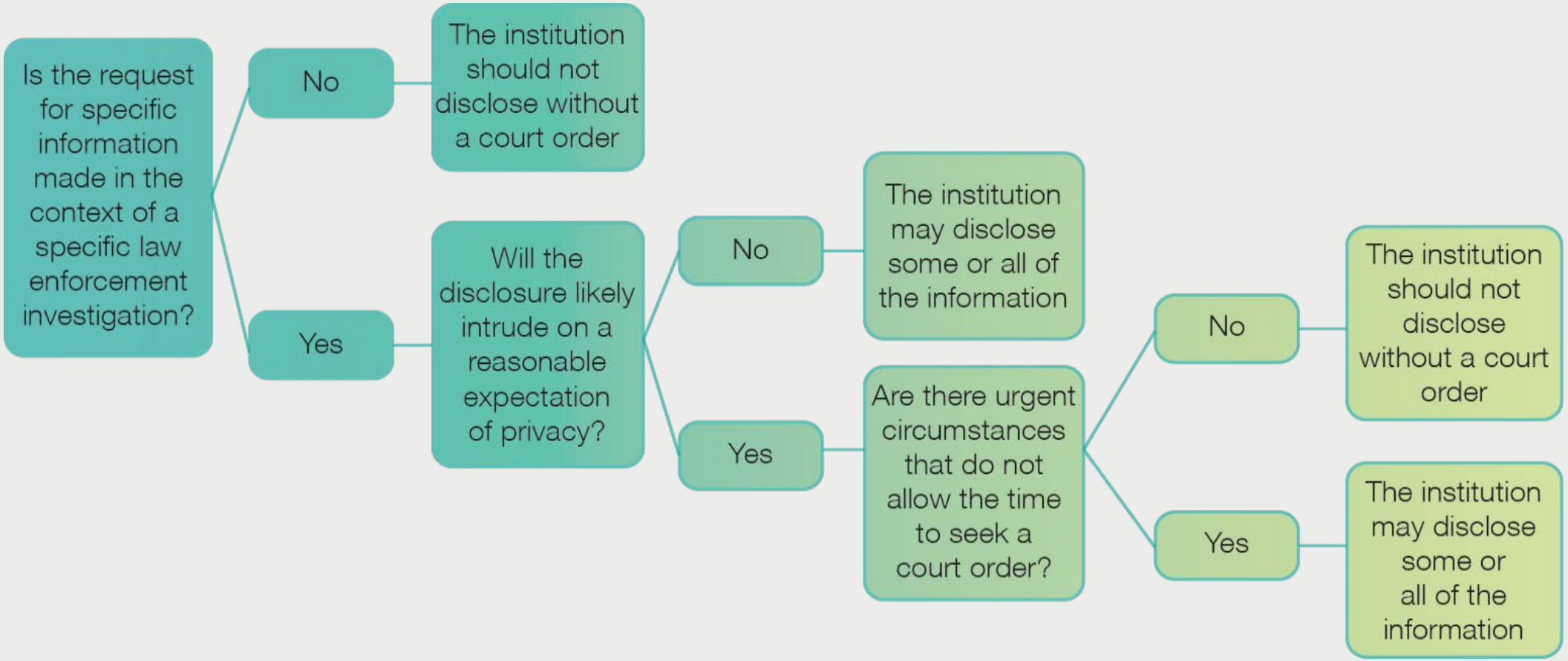
Generally, institutions should disclose personal information to a law enforcement agency *only when required by law*, such as in response to a court order, rather than a simple request, where there is no requirement to disclose.

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.

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

Law Enforcement Investigations



Cyberattacks

Systems infected by:

- phishing schemes to gain access to passwords/information
- ransomware and other software exploits used to gain control of computer systems

Statement from the Town of Wasaga Beach regarding the ransomware attack on the municipality's servers

Wasaga Beach – The Town of Wasaga Beach computer system was subject to a ransomware attack on Sunday, April 29, 2018.

The attack encrypted the town's servers, locking out access to the data
These servers contain all the town's data, including
on the town's infrastructure

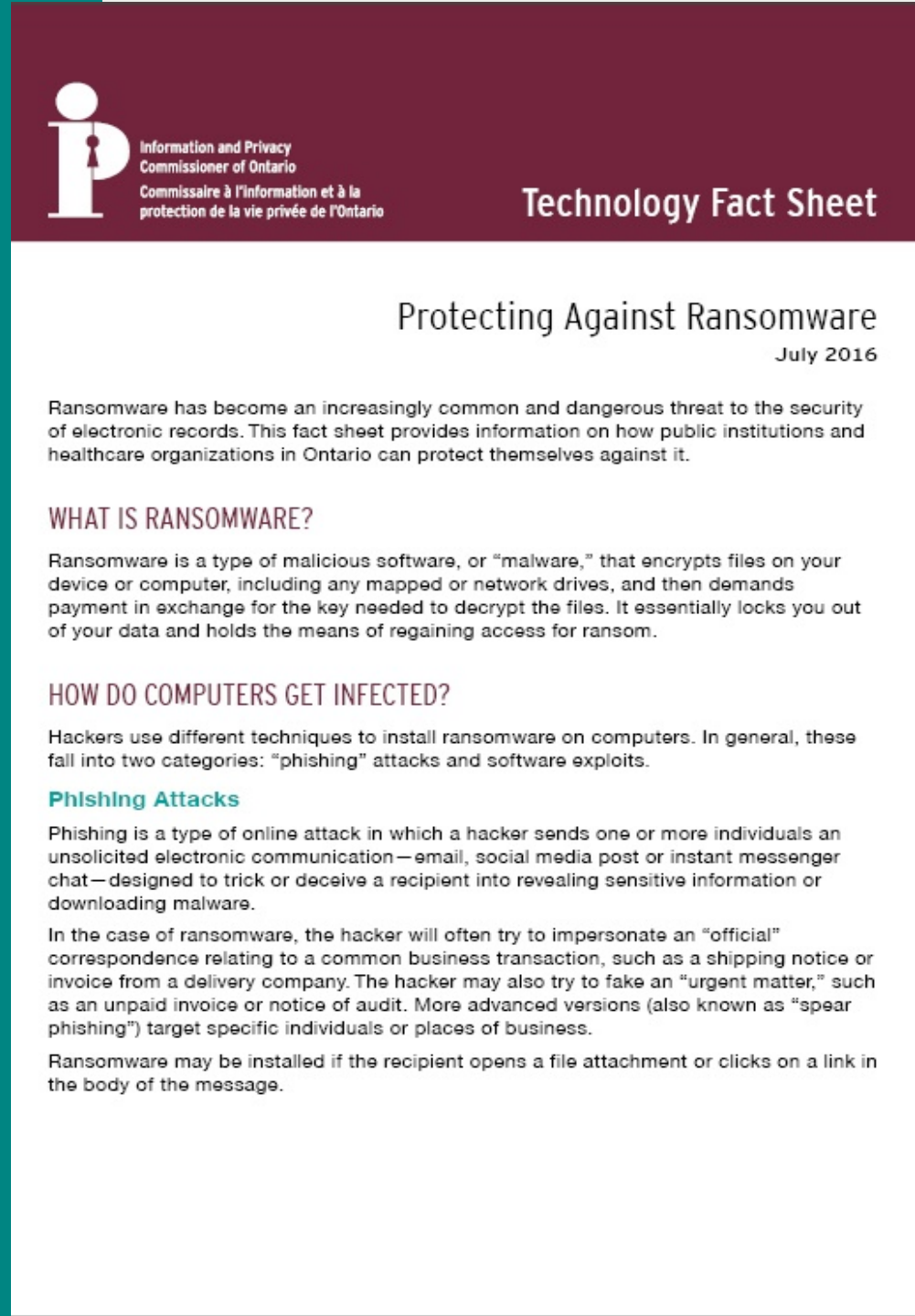
Ontario police warn of recent cyberattacks targeting local governments

THE CANADIAN PRESS Updated: September 14, 2018

Ransomware

Protect your organization

- Train employees
- Limit user privileges
- Use software protections and back-ups
- Have an incident response plan in place



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.

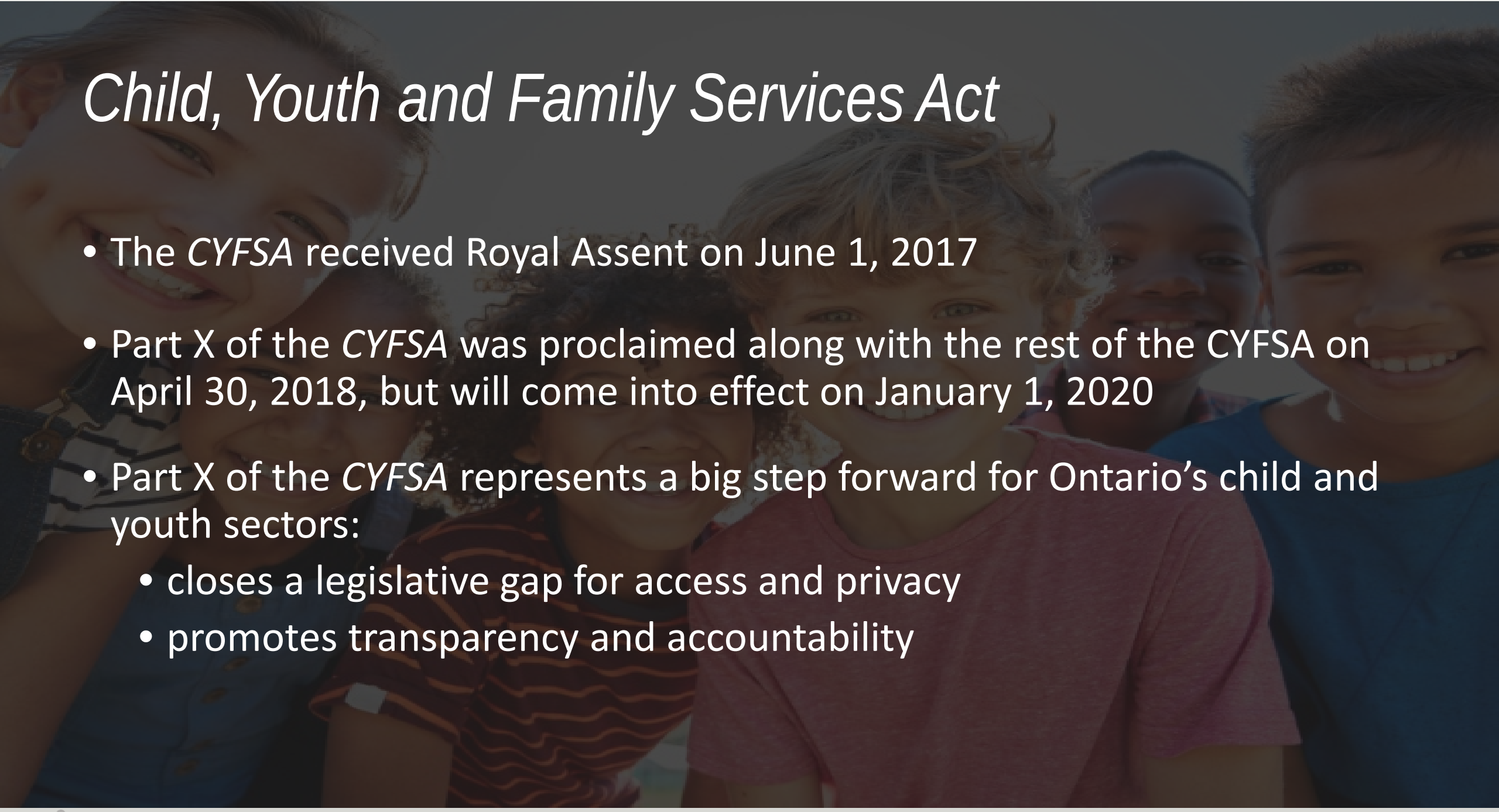
Phishing Attacks

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.

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

IPC Fact Sheets

- Published in response to frequently asked questions about access, privacy and technology
- Recently released:
  - Fees, Fee Estimates and Fee Waivers
  - Frivolous and Vexatious Requests
  - Disposing of Your Electronic Media

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

IPC Webinars

- The webinar series has helped us to overcome geographical barriers and engage with Ontarians, regardless of where they live or work
- Registrants watch a live presentation and participate in a QA session.
- Past webinar presentations on our website

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