

# *Privacy and Access Rights and Obligations under MFIPPA*

Renee Barrette  
Director of Policy

Ayesha Kapadia  
Policy Analyst

Office of the 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

OACA 2021 Virtual  
Conference

June 8<sup>th</sup>, 2021

# IPC's Mandate

- *Freedom of Information and Protection of Privacy Act (FIPPA)*
  - covers 300 provincial institutions
- *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*
  - covers 1,200 municipal organizations
- *Personal Health Information Protection Act (PHIPA)*
  - covers individuals and organizations involved in the delivery of health care services
- *Child, Youth and Family Services Act (Part X) (CYFSA)*
  - children's aid societies, child/youth service providers



Freedom of Information

Right of access

# Access to Information: A Pillar of Democracy

“The overarching purpose of access to information legislation... is to facilitate democracy.”

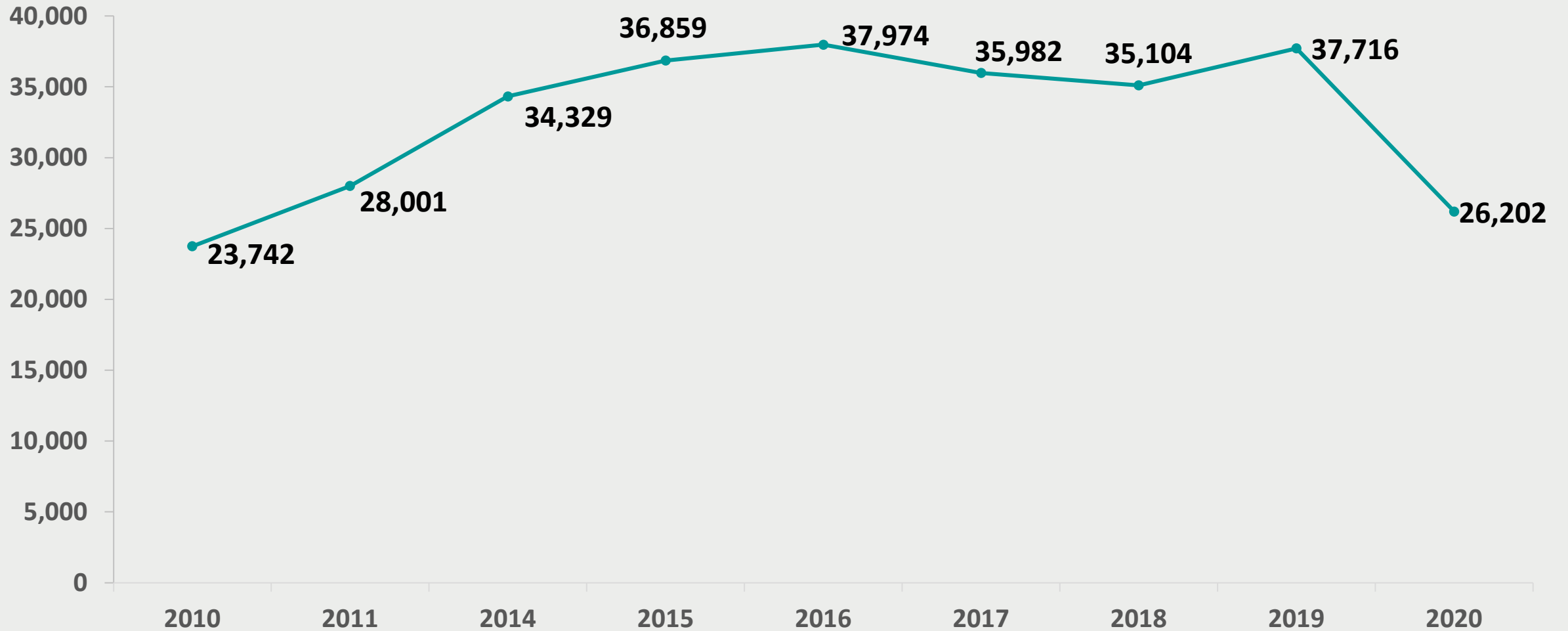
SCC Justice La Forest

*Dagg v. Canada (Minister of Finance)*, 1997

# Right of Access Under *M/FIPPA*

- Every person has a **right of access** to a record in the custody/control of an institution, with limited exceptions
- Any person can:
  - ask for their own information
  - ask for general records
  - request a correction of their personal information
- Any record can be requested (the question “Is this FOI-able” is a common one)
  - paper records, emails, videos, photos, electronic information

# Access Requests Filed Under *MFIPPA*



# *MFIPPA* Exemptions: Limited and Specific

## DISCRETIONARY EXEMPTIONS INCLUDE

- draft by-laws (s.6)
- advice and recommendations (s.7)
- law enforcement (s.8)
- relations with other governments (s.9)
- relations with Aboriginal communities (s.9.1)
- economic interests (s.11)
- solicitor-client privilege (s.12)
- danger to safety or health (s.13)

## MANDATORY EXEMPTIONS

- third party information (s.10)
- someone else's personal information (s.14)

# IPC Appeals

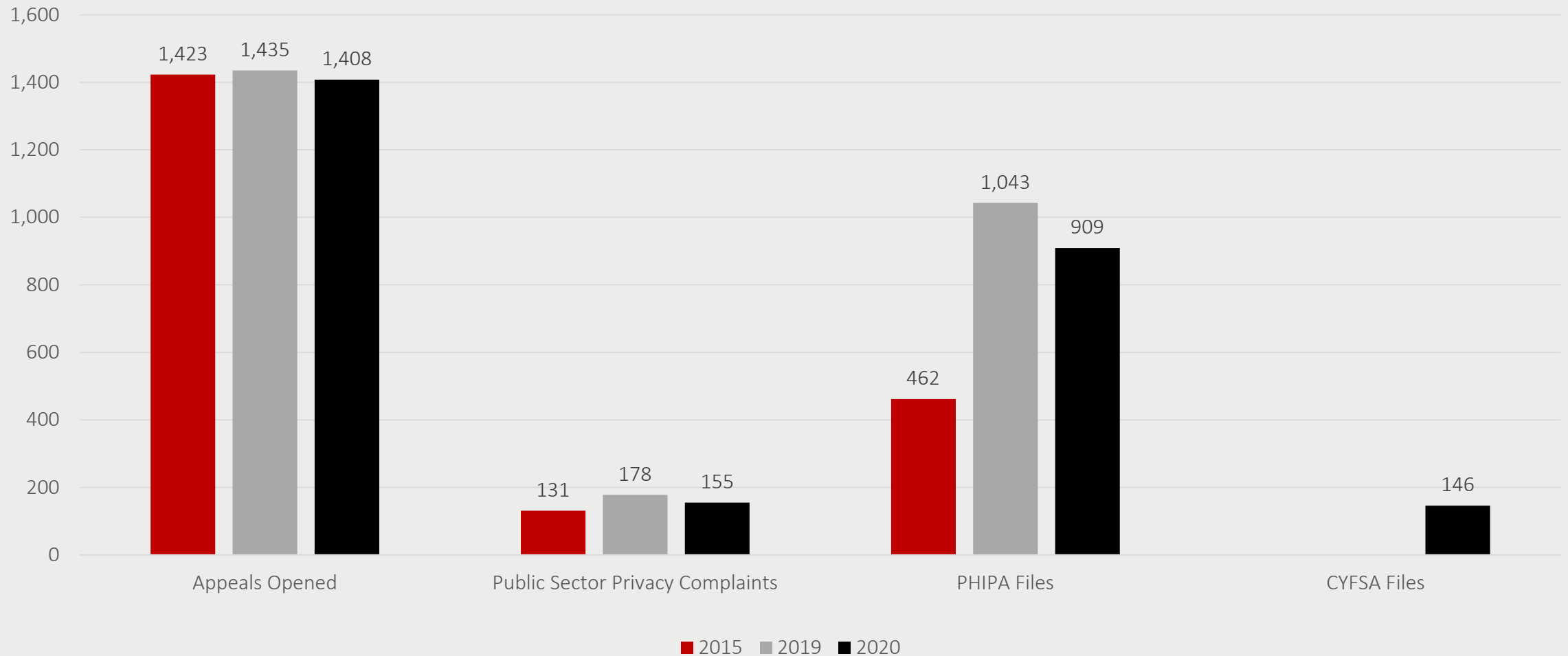
A requester may appeal **any decision** of the institution, including:

- denial of access
- fees
- failure to provide timely decision or conduct a reasonable search
- extending the time for a decision beyond the 30 days
- denying a correction request

A third party may appeal the institution's decision to disclose information that affects their interests

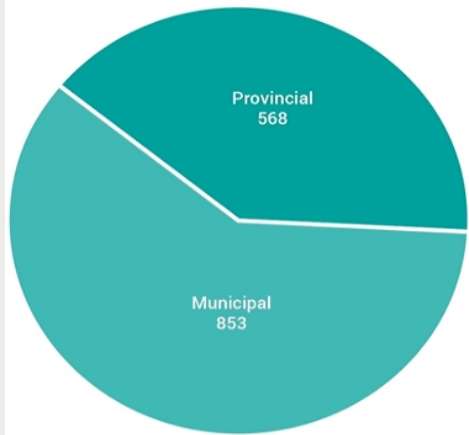


# Appeals, Complaints and Breaches

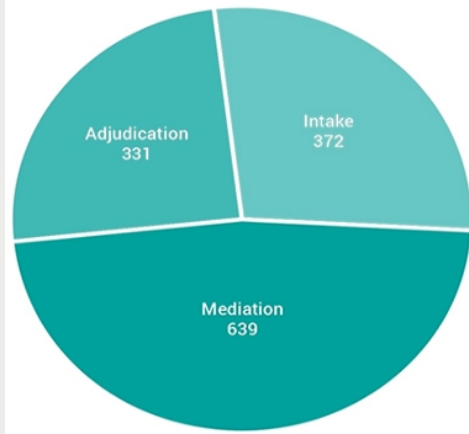


# Appeals for 2019

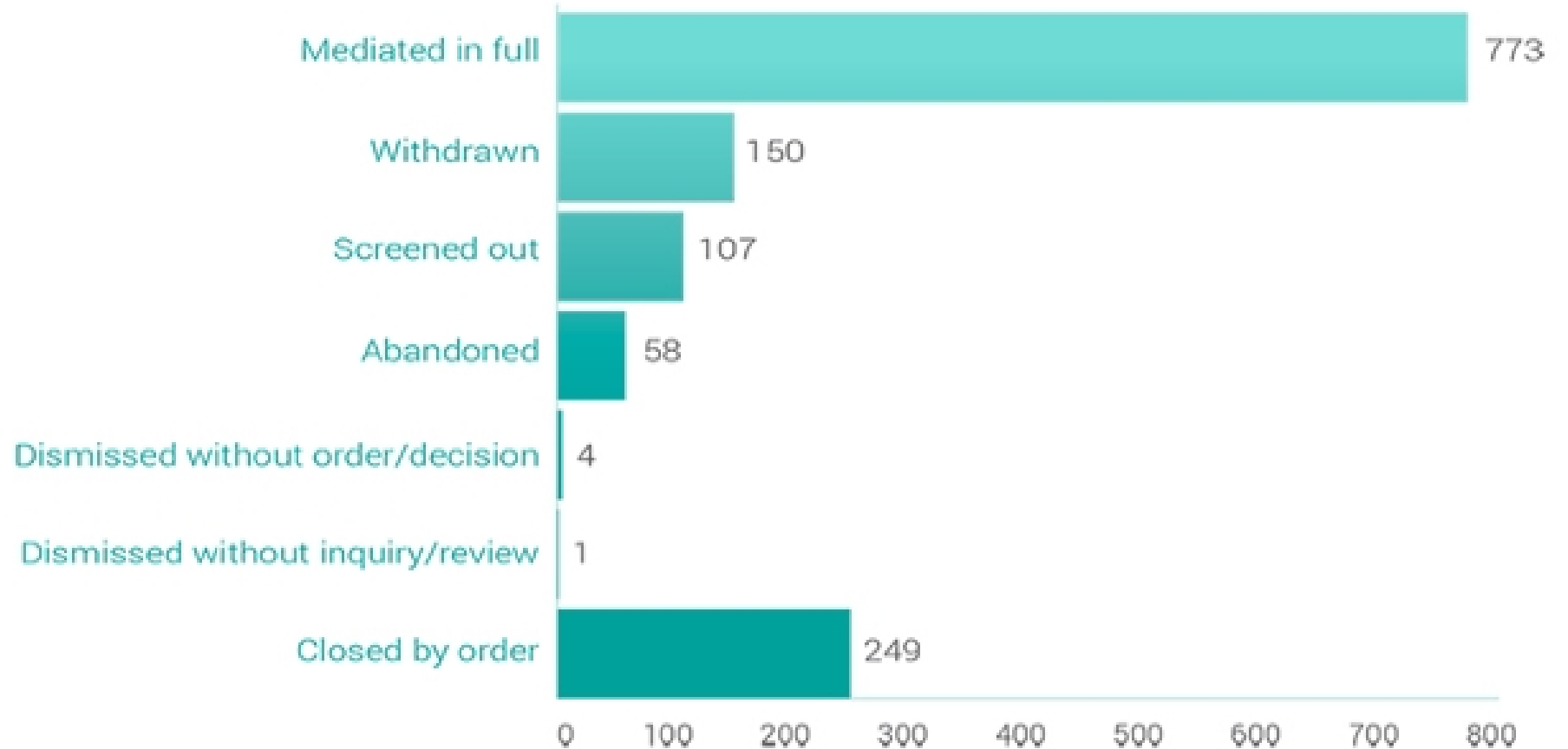
ACCESS APPEALS RECEIVED



APPEALS RESOLVED BY STAGE



OUTCOME OF APPEALS






# Protection of Privacy

# What is Personal Information?

- **Personal information** means recorded information about an identifiable individual:
  - even without a name, it may be personal information if the individual can be identified
- **Record** means a record of information in any form:
  - includes electronic records, paper records, audio and video recordings, etc.



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.

# Privacy Obligations Under *M/FIPPA*

*M/FIPPA* protects **privacy** through rules for the collection, use, disclosure of personal information

No **collection** unless

- authorized by statute
- used for law enforcement
- 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 licence

# Privacy Obligations Under *M/FIPPA*

.....

No **use** of personal information unless

- for purpose collected
- for consistent purpose
- with consent

A university can use personal information it collected to identify and notify students who may qualify for a scholarship offered by nonprofit organizations

.....

No **disclosure** unless

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

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

# Security Obligations

*MFIPPA* s. 3(1) of Regulation 823:

- Requires institutions to ensure that **reasonable measures** are defined, documented and put in place, taking into account the nature of the records to protect, to prevent:
  - unauthorized access to records in their custody or control

# Privacy Breaches

- **Privacy breaches** occur when personal information is collected, used, disclosed in ways not authorized by the acts
  - can be deliberate: police officer looks up ex-girlfriend's information on CPIC
  - or accidental: mass mailing containing health card renewal notices goes to wrong recipients because of technology glitch
- IPC may **investigate** privacy complaints, report publicly on them
  - may order government to cease and destroy an improper collection of personal information
  - may make recommendations to safeguard privacy



# Responding to a Privacy Breach

## STEP 1: Immediately Implement Privacy Breach Protocol

- ❖ Notify all relevant staff, develop and execute plan to contain the breach and notify those affected, contact the IPC and provide details of what happened

## STEP 2: Stop and Contain the Breach

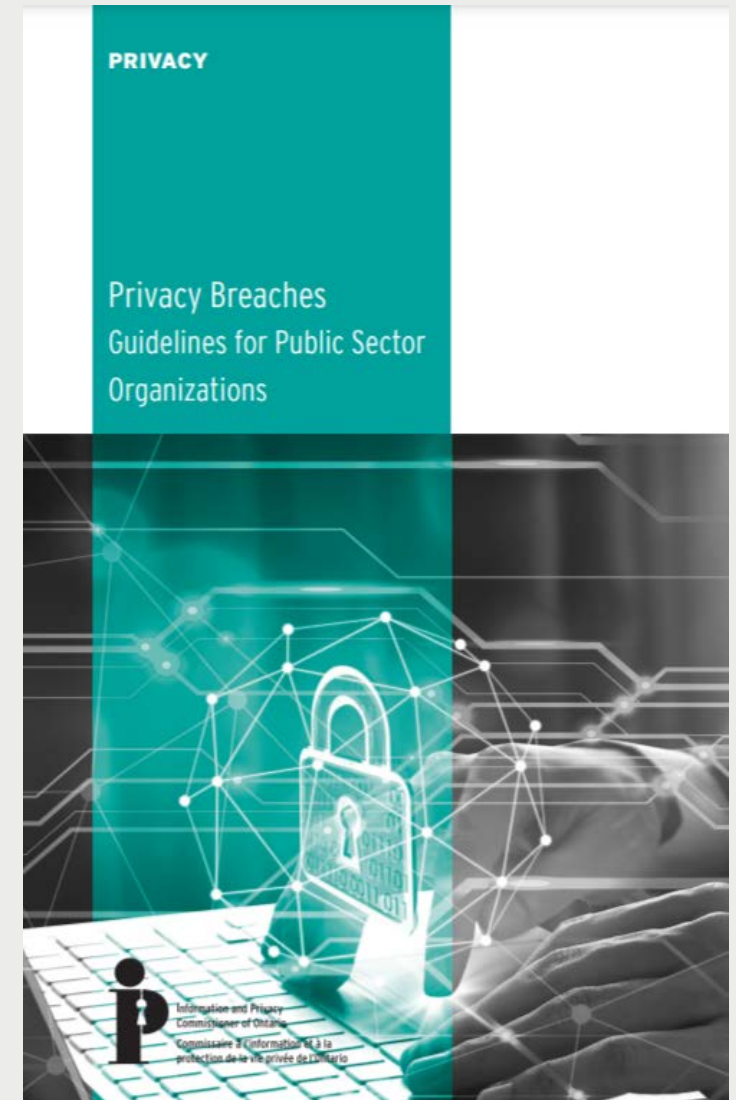
- ❖ Identify the scope of the breach and take necessary steps to contain it

## STEP 3: Notify Those Affected by the Breach

- ❖ Take necessary steps to notify individuals whose privacy has been breached at the first reasonable opportunity

## STEP 4: Investigation and Remediation

- ❖ Conduct an internal investigation



# Best Practices in Protecting Privacy

- **Limit** amount of personal information collected and used
- Ask whether it is **necessary** to use personal information to get the work done
  - e.g. necessary to name individuals in briefings? Are all personal details necessary?
- **Protect** personal information from deliberate or accidental unauthorized use or disclosure



# Recent Decisions and Resolutions

# Custody and Control

Personal email accounts of elected officials

- **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 councilor
- 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

# Third Party Information & Public Interest Override

## Ottawa's Light Rail Transit Project

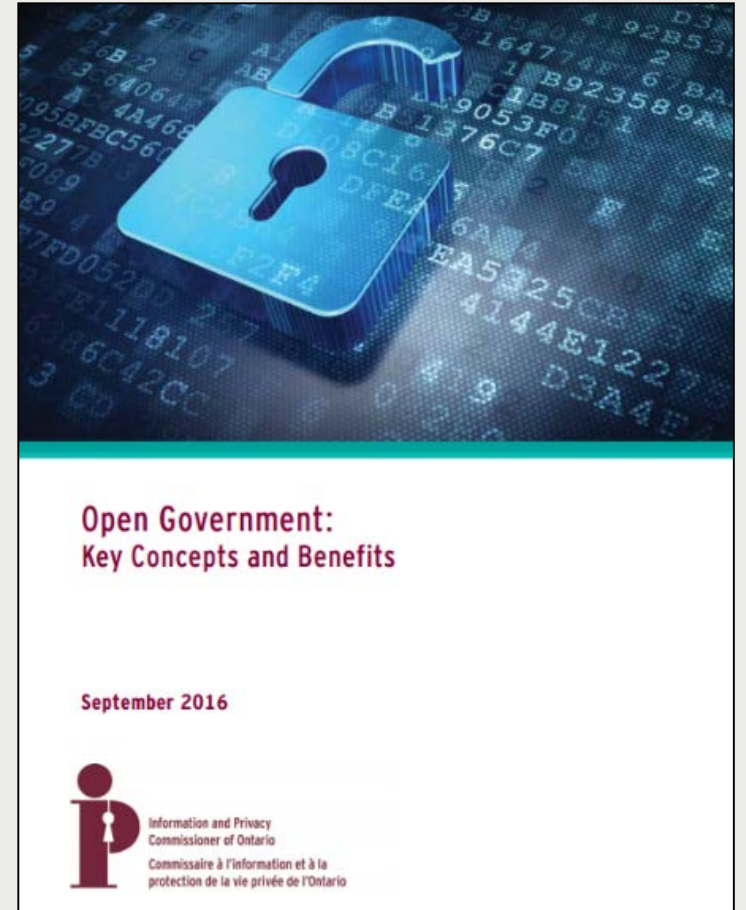
- **MO-3628:** The City of Ottawa received a request for all “non-conformance reports” issued in 2015/16 referencing below standard construction on phase one of the project.
- The city granted access in part, claiming the mandatory **third-party exemption** (s.10(1) *MFIPPA*): the information was technical information, supplied in confidence by the third party to the city, giving rise to a likelihood of harm (prejudice to the third party's competitive position).
- The adjudicator found that the non-conformance reports were indeed exempt from disclosure under s. 10(1), but that the **public interest override** applied to these records, which were disclosed to the appellant
- Two-part test for **public interest override**:
  1. there must be a compelling public interest in the disclosure, and
  2. this interest must clearly outweigh the purpose of the exemption



Guidance

# Open Government: Key Concepts and Benefits

- IPC's introductory guidance summarizes fundamental concepts and benefits, draws together variety of sources to facilitate understanding of Open Government
- Highlights two significant goals:
  1. **Enhancing transparency** to improve the quality of governance and services by becoming more open, accountable, and responsive to the public
  2. **Enhancing public engagement** to enable broad participation and true two-way dialogue, resulting in more “citizen centric” information and services



# Open Government and Protecting Privacy

- Guidance issued to assist institutions with enhancing proactive disclosure while ensuring protection of privacy
- Helps institutions understand that privacy is not a barrier to Open Government and that proactively addressing privacy risks is critical to the success of any open government initiative





# Open Government: Key Implementation Considerations

- Overview of important considerations when implementing Open Government
- Key factors for success:
  - recognizing Open Government is an **ongoing program**, not short-term project
  - making sure institution has **leadership**, commitment, governance, resources to sustain program
  - defining scope and **deliverables** realistically, appropriate for institution
  - **engaging** users and public as institution plans, implements and evaluates its activities and services



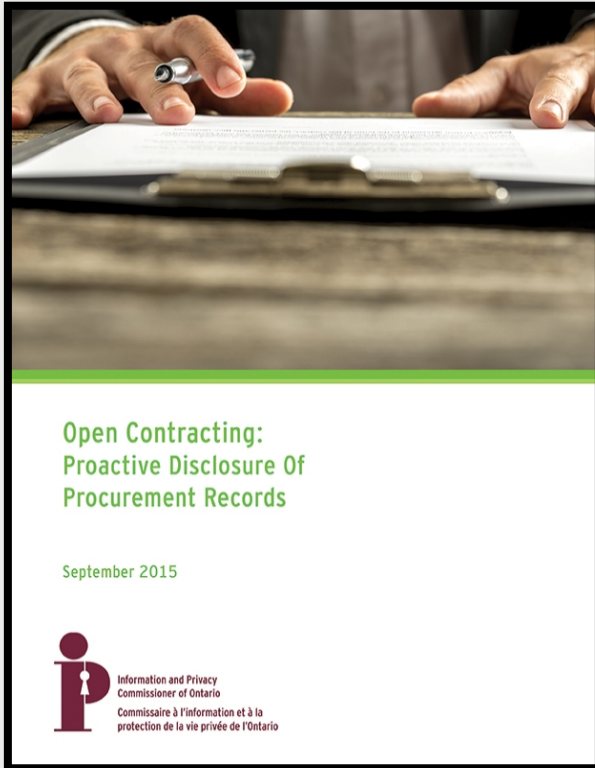
# Open Government - Proactive Disclosure

- Open Government supports, expands *M/FIPPA* right of access; more than just reactive disclosure (in response to access request)
- Government information should be made public in anticipation of, and in response to, the **public's needs and interests**, unless there are legitimate legal, privacy, security, confidentiality reasons not to
- **Open by Default** is a **presumption** in favour of disclosure over non-disclosure, mirrors *M/FIPPA's* over-arching access principles

## Three pillars:

1. **Open Data**: proactive publication of data in free, accessible forms for public use (e.g. water test results)
2. **Open Dialogue**: new ways to provide public with a meaningful voice in planning, decision making (e.g. police carding consultations, e-petitions)
3. **Open Information**: proactive release of information about the operation of government (e.g., contracts)

# 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**

# Key Benefits

## Enhanced Accountability

- strengthens democracy by making government more **accountable** for its decisions, actions, spending

## Enhanced Public Participation

- public has **stronger voice**, ability to influence government
- empowers public to make better decisions impacting quality of life

## Enhanced Economic Value

- increased use of government information supports **innovation**, creates **economic opportunities** that benefit business, government, public

# De-identification Supports Open Government

- “De-identification” - process of removing PI from a record or data set
- Outlines a risk-based, step-by-step process to assist institutions in de-identifying data sets containing PI
- Covers key issues to consider when publishing data:
  - *release models*
  - *types of identifiers*
  - *re-identification attacks*
  - *de-identification techniques*



## De-identification Guidelines for Structured Data

June 2016

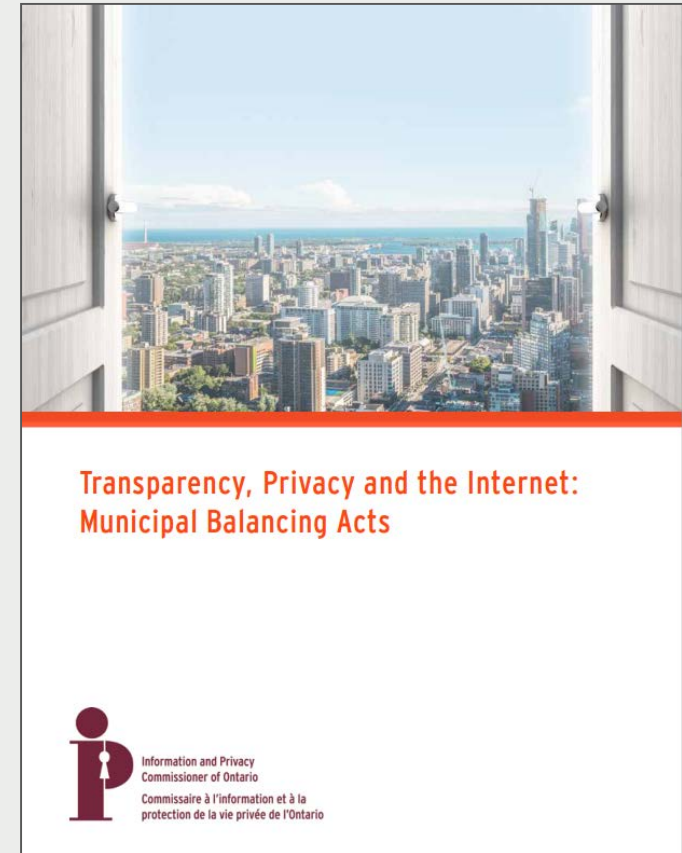


# Publishing on the Internet – Privacy Complaint MC13-67

- A complaint was received about a municipality's online publication of **personal information** collected as part of a minor variance application
- IPC found that the publication of this information was **not in contravention** of the *M/FIPPA* because the published information was required to be made publicly available under the *Planning Act*
- IPC however, recommended that the City consider implementing privacy protective measures that obscure this type of information from search engines and automated agents

# Publishing on the Internet IPC Guidance

- Guide provides municipalities with **privacy protective policy, procedural** and **technical** options when publishing personal information online
- Focus is primarily on personal information that is required by legislation to be published, but **may be applied** in any situation where municipalities make information available online



# Publishing on the Internet

Privacy protection may be improved through a number of risk mitigation strategies:

- **Redaction**
  - remove unnecessary personal information before publishing
- **Data minimization**
  - request and store only as much personal information as is necessary
- **Technological measures to limit searchability**
  - e.g. robot exclusion protocols, images instead of text
- **Transparent administration**
  - when information received, be clear about how it will be published; manage expectations



# Examples from Public Institutions Across Canada

- The [Canadian Human Rights Tribunal](#), the [Social Security Tribunal](#) and the [Manitoba Labour Board](#) replace names with initials when they post decisions online.
- The [Canada Agricultural Review Tribunal](#) and the [Public Service Labour Relations and Employment Board](#) use sitemaps that exclude web pages and directories containing personal information, hiding that content from robots.
- The [Ontario Government Open Data Portal](#) uses JavaScript to disguise the website's navigation structure from robots since very few are able to execute that programming language.

The background is a solid teal color. On the left side, there is a large, semi-transparent green shape that resembles a speech bubble or a stylized speech bubble tail pointing downwards and to the left. The text "New Challenges" is centered within this green shape.

New Challenges

# Ontario city of Burlington out \$503,000 after staff member falls for phishing scam

*They say the staff member made a single transaction to a 'falsified bank account' after receiving an email requesting to change banking information*

# PHISHING SCAM LEADS TO SUSPENSION OF ONLINE ACCESS FOR HUNDREDS OF STAFF ACCOUNTS

February 13, 2019 | By Joshua Ambar

[Facebook](#)
[Twitter](#)
[Google+](#)
[LinkedIn](#)
[Pinterest](#)

Algonquin was hit with yet another cyber attack on Tuesday, Jan. 29, when hundreds of employees opened a... as if President Cheryl Jensen sent it.

## Canadian Underwriter

YOUR GUIDE TO INSURANCE SUCCESS. SINCE 1934

News

### Cyber attack in Canada spawns \$60 million lawsuit

March 29, 2019 by By Colin Perkel - THE CANADIAN PRESS

[Print this](#)
[Share](#)

TORONTO - As many as 200,000 people may have had their personal information stolen in a hack on servers at one of Ontario's most popular casinos, a lawyer for the plaintiffs press proposed class action argued on Thursday.

However, a lawyer for Casino Rama countered that, at most, 10,000 to 11,000 people were victimized and the plaintiffs' definition of who should be included in the proposed class action was far too broad.

news Ontario police warn of recent cyberattacks targeting local governments

Toronto

### Ontario police warn of recent cyberattacks targeting local governments

[Facebook](#)
[Twitter](#)
[Email](#)
[Reddit](#)
[LinkedIn](#)

Attacks launched through direct hacking into vulnerable systems or through phishing emails, OPP said

news Eastern Ontario community hit with ransomware attack

Ottawa

### Eastern Ontario community hit with ransomware attack

[Facebook](#)
[Twitter](#)
[Email](#)
[Reddit](#)
[LinkedIn](#)

The Nation, Ont., has computer networks frozen in online attack

CBC News - Posted: Jul 08, 2019 8:37 PM ET | Last Updated: July 9



The municipality had its computer networks frozen by the hack. (Brian Jackson/Shutterstock)

news Ottawa Hospital targeted by cyberattack

Ottawa

### Ottawa Hospital targeted by cyberattack

[Facebook](#)
[Twitter](#)
[Email](#)
[Reddit](#)
[LinkedIn](#)

Hackers target four computers but no data compromised, says hospital

The Canadian Press - Posted: Mar 13, 2016 9:26 AM ET | Last Updated: March 13, 2016



The Ottawa Hospital on Carling Avenue on Jan. 22, 2016. (Michel Aspirot/CBC)

The Ottawa Hospital says it was the subject of a cyberattack over the past week.

The hospital issued a statement Saturday saying four of the hospital's 9,800 computers faced a hacker attempt, but no patient information was affected.

# Working from Home

New IPC publication to serve as guidance for employees working from home

Includes best practices for adopting virtual communication channels while protecting personal information and responsibly managing data

Staff must be reminded of responsibilities to:

- follow all information security protocols
- remain vigilant of phishing attacks
- immediately report any data breaches
- properly preserve and catalogue records so they can be found when responding to access requests

## Working from home during the COVID-19 pandemic

Many government and public sector organizations had to close their offices with little advance notice because of the public health crisis brought on by COVID-19. People are working from home, many in makeshift conditions that were never planned or anticipated. This creates the potential for new challenges and risks to privacy, security, and access to information

Although this is an unprecedented and rapidly changing situation, Ontario's access and privacy laws continue to apply. As a result, your organization must take timely and effective steps to mitigate the potential risks associated with this new reality. This fact sheet outlines some best practices to consider when developing a work-from-home plan that protects privacy and ensures access to information.

### WORK FROM HOME POLICIES

You should work with your information technology, security, privacy, and information management staff to review and update any existing work-from-home policies to adequately address the risks to access, privacy and security, as they may have evolved since originally drafted.

If you do not have such policies in place, you should create them by adapting your existing privacy, security, and data access policies to the unique features of the current context where virtually everyone is working from home.

# Phishing

Guides public institutions on how to protect personal information from phishing attacks

- What is phishing?
- Impacts of phishing attacks
- How to recognize phishing messages
- How to protect against phishing attacks
- How to respond to phishing attack



## Protect Against Phishing

Phishing is a common method hackers use to attack computer systems. Successful phishing attacks pose a serious threat to the security of electronic records and personal information.

Ontario's privacy laws require public and healthcare organizations to have reasonable measures in place to protect personal information in their custody or control.

Phishing attacks pose a serious threat to the security of electronic records and personal information

### WHAT IS PHISHING?

Phishing is a type of online attack in which an attacker — using both technological and psychological tactics — sends one or more individuals an unsolicited email, social media post, or instant message designed to trick the recipient into revealing sensitive information or downloading malware.

Malware (malicious software) is any software intentionally designed to disrupt, damage, or gain unauthorized access to a computer system.

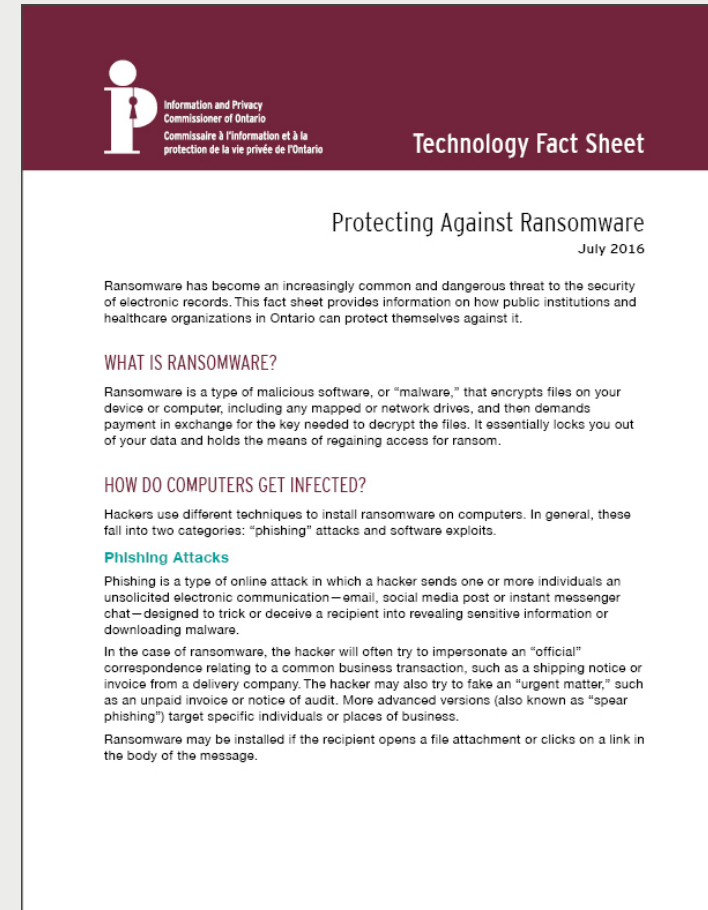
Phishing attacks can be generic or customized, and can target both individuals and entire organizations. Attacks that target a specific individual or organization are commonly referred to as spear phishing attacks.

The main goal of a phishing attack is to get the individual to do something that compromises the security of their organization. Attackers achieve this when recipients:

- reply to phishing emails with confidential information

# Protecting Against Ransomware

- High-level summary of issues
- What is ransomware?
- How do computers get infected?
  - Phishing attacks
  - Software exploits
- Protecting your organization
- Responding to incidents





What Lies Ahead?

# *M/FIPPA* Reform

- In the thirty years since *M/FIPPA* was enacted there have been significant changes in public expectations, technology, and the ways in which government does business
- IPC has repeatedly called for a comprehensive review of *M/FIPPA* in order to update the acts and ensure that access and privacy rights of Ontarians are protected
- Recommendations include:
  - expanding coverage of the acts to include arms-length agencies, delegated administrative authorities, self-funded agencies etc.
  - amendments to address changes in communication and information technology
  - expanding the Commissioner's order-making powers
  - mandatory proactive disclosure of identified categories of records



# Made-in-Ontario Private Sector Privacy Law

- August 13 – Ministry of Government and Consumer Services launched a consultation to explore whether the time has come for a made-in-Ontario private sector privacy law
- Government’s consultation paper discussed:
  1. increased transparency
  2. clear consent provisions
  3. right to deletion and de-indexing
  4. data portability
  5. compliance and enforcement
  6. de-identified and derived data
  7. expanded scope to include non-commercial organizations
  8. data sharing including through data trusts

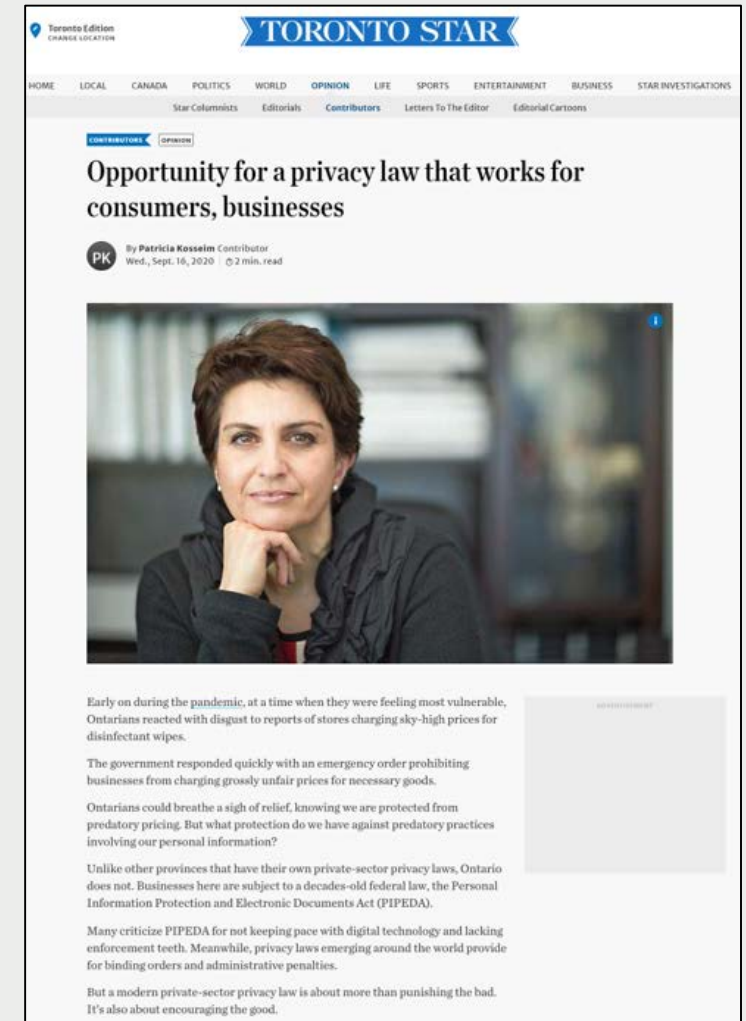
# Ontario's Opportunity in a Nutshell

- A provincial private sector privacy law could:
  - provide more comprehensive protection in areas where the federal government is constitutionally constrained from acting
  - be better suited to the realities of small and medium sized enterprises
  - provide a more seamless regulatory regime for innovative, intersectoral initiatives specific to Ontario
  - fill an important void for vulnerable populations, including children

# IPC Support for Private Sector Privacy Law

Key elements of a modern privacy framework:

- enhanced transparency and accountability requirements
- an emphasis on individual privacy rights, with clear rules for meaningful consent and pragmatic exceptions to consent subject to protective guardrails
- an agile regulator with the modern tools needed to support responsible innovation
- a broad range of enforcement mechanisms



- [Read Op-Ed](#)



# IPC's Strategic Priority-Setting Exercise

## Goal:

- Identify access and privacy priorities

## Why:

- Prioritize the most pressing access and privacy challenges for Ontarians
- Focus and leverage resources
- Guide *discretionary* decision-making
- Enhance positive impact



# IPC's Strategic Priorities 2021-2025

## Privacy and Transparency in a Modern Government

**Advance** Ontarians' privacy and access rights by working with public institutions to develop bedrock principles and comprehensive governance frameworks for the responsible and accountable deployment of digital technologies

## Children and Youth in a Digital World

**Champion** the access and privacy rights of Ontario's children and youth by promoting their digital literacy and the expansion of their digital rights while holding institutions accountable for protecting the children and youth they serve

## Next-Generation Law Enforcement

**Contribute** to building trust in law enforcement by working with relevant partners to develop the necessary guardrails for the adoption of new technologies that protect both public safety and Ontarians' access and privacy rights

## Trust in Digital Health

**Promote** confidence in the digital health care system by guiding custodians to respect the privacy and access rights of Ontarians, and supporting the pioneering use of personal health information for research and analytics to the extent it serves the public good



## Privacy and Transparency in a Modern Government

Advance Ontarians' privacy and access rights by working with public institutions to develop bedrock principles and comprehensive governance frameworks for the responsible and accountable deployment of digital technologies.



## Trust in Digital Health

Promote confidence in the digital health care system by guiding custodians to respect the privacy and access rights of Ontarians, and supporting the pioneering use of personal health information for research and analytics to the extent it serves the public good.



Accessibility & Equity

Collaboration & Consultation

Vision & Pragmatism

Knowledge Development

## Children and Youth in a Digital World

Champion the access and privacy rights of Ontario's children and youth by promoting their digital literacy and the expansion of their digital rights while holding institutions accountable for protecting the children and youth they serve.



## Next-Generation Law Enforcement

Contribute to building public trust in law enforcement by working with relevant partners to develop the necessary guardrails for the adoption of new technologies that protect both public safety and Ontarians' access and privacy rights.





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](http://www.ipc.on.ca)

E-mail: [info@ipc.on.ca](mailto:info@ipc.on.ca)

Media: [media@ipc.on.ca](mailto:media@ipc.on.ca) / 416-326-3965