Access and Privacy in Ontario: A Primer

Eric Ward, Assistant Commissioner

Gillian Shaw, Director of Adjudication

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

Political Staff Training

September 23, 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
- *Anti-Racism Act (ARA)*
  - oversight of the privacy protective rules

Freedom of Information

Right of access under *FIPPA*

Access to information: A pillar of democracy

"The overarching purpose of access to information legislation… is to facilitate democracy."

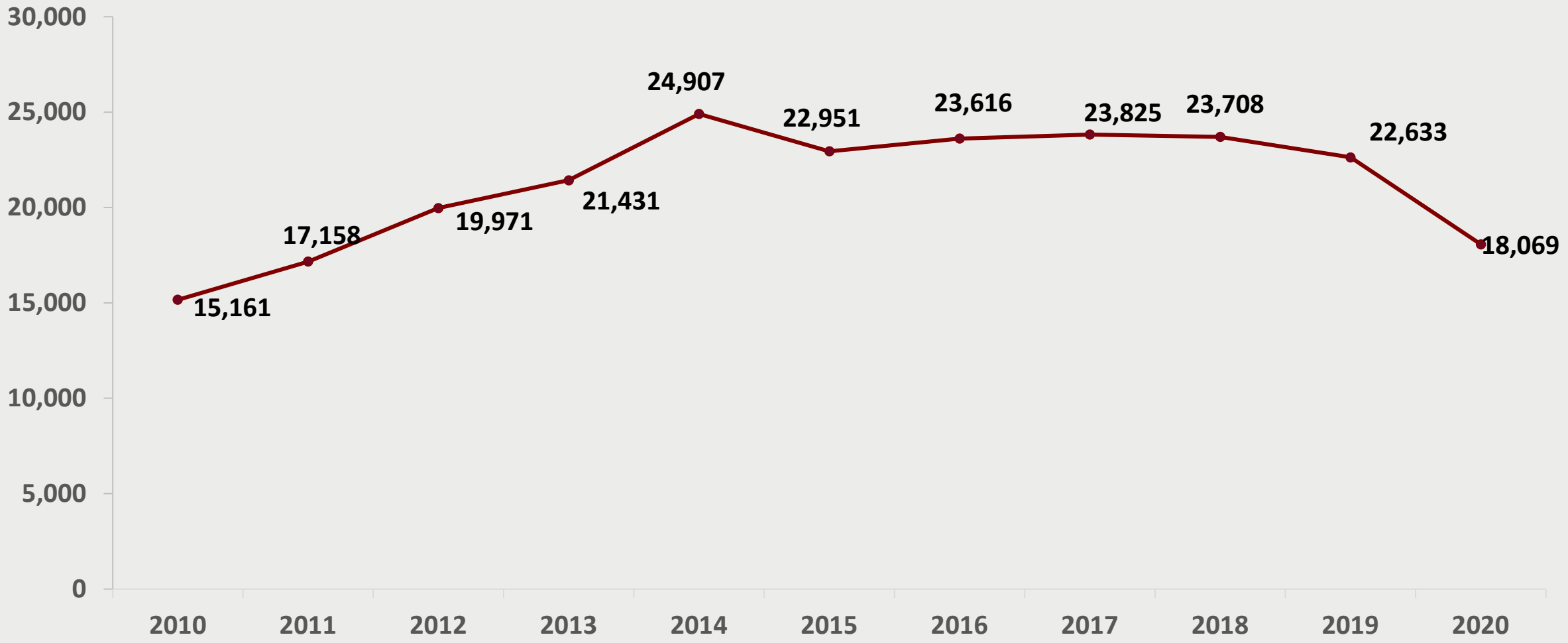
SCC Justice La Forest

Dagg v. Canada (Minister of Finance), 1997

Right of access under *FIPPA* and *MFIPPA*

- Every person has a right of access to a record in the custody/control of an institution, with limited exceptions
- A person making a request does not need to have a reason for requesting records
- Any person can:
  - ask for their own information
  - ask for general records
- Any record can be requested ("Is this FOI-able?" is a common question)
  - paper records, emails, videos, photos, electronic information
  - the institution typically has 30 days to respond to a request by granting access or applying an exemption or exclusion

Access requests filed under *FIPPA*



Exemptions from the right of access: Limited and specific

Examples of exemptions

- advice or recommendations (s.13)
- law enforcement (s.14)
- relations with other governments (s.15)
- relations with Aboriginal communities (s.15.1)
- economic interests (s.18)
- solicitor-client privilege (s.19)
- danger to safety or health (s.20)
- cabinet records (s.12)
- third party information (s.17)
- someone else's personal information (s.21)

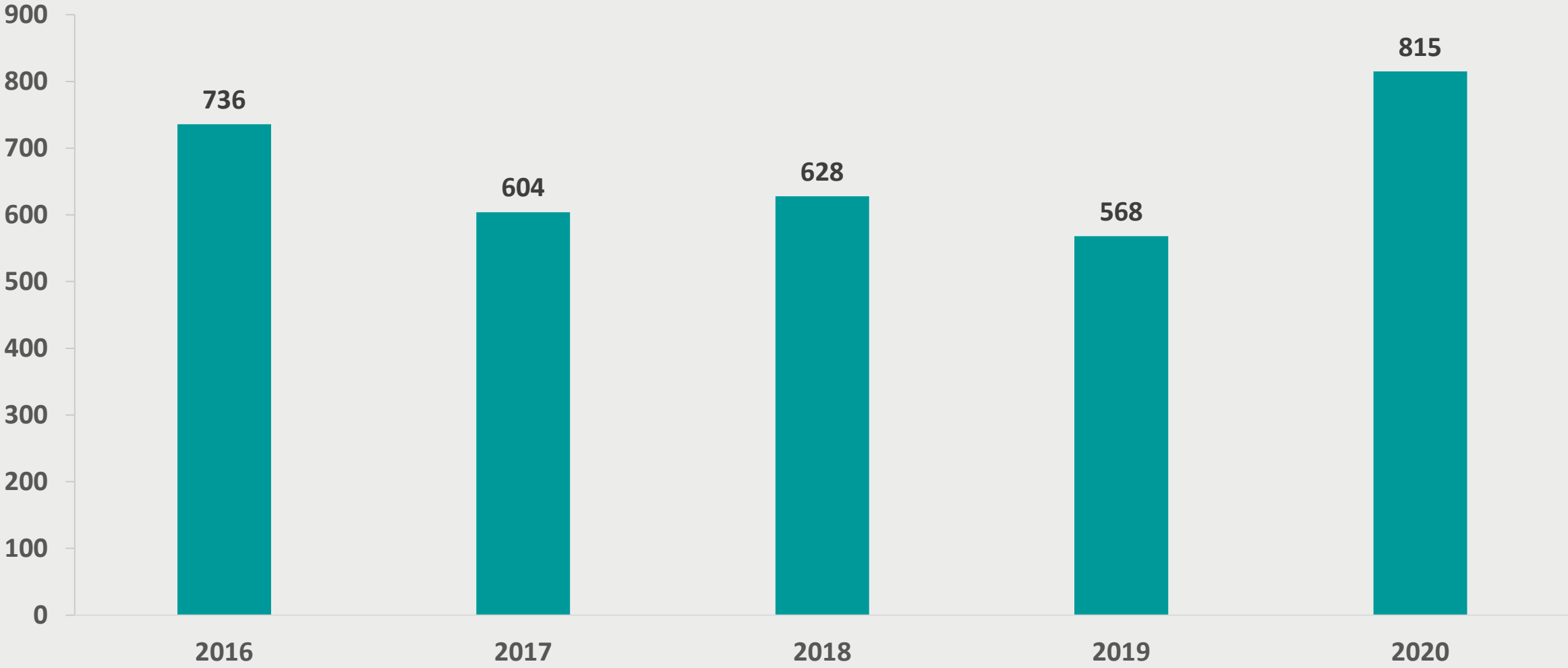
Public interest override (s. 23)

- can result in releasing records even if they are exempt under one of the exemptions

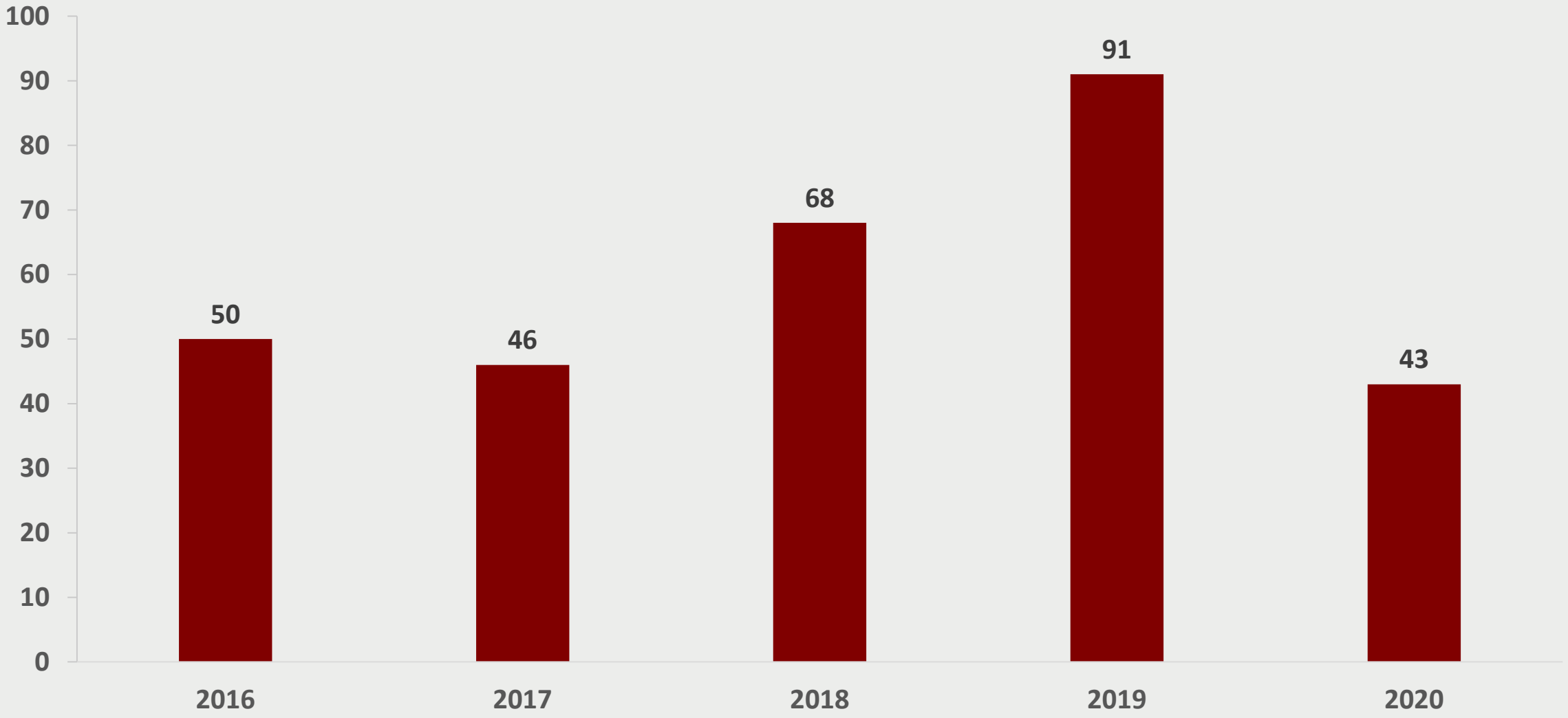
IPC appeals

- A requester may appeal any decision of an institution, including denial of access
- A third party may appeal the institution's decision to disclose information that affects their interests

Provincial access appeals opened



Provincial public sector self-reported privacy breaches



IPC Order PO-4165: Deemed refusal

- Public Health Ontario (PHO) received two requests for emails relating to lab testing capacity and the coronavirus
- PHO did not respond in the required 30 days, applied time extension to both requests without specifying length of time, citing impact of pandemic on its operations
- IPC found PHO to be in a “deemed refusal” situation and ordered PHO to issue access decisions within specified time

Questions on FOI process?

Political party and constituency records

- Political party and constituency records generally fall outside the scope of *FIPPA*
- Good idea to ensure these records are stored separately from government files
- If mixed, can be difficult to differentiate them from government files
- Even where a record is sent from or received by political or personal email account, if it relates to information about the business of the institution, it may fall under *FIPPA*

IPC Order MO-3471: Political records – no custody or control

- Request for access to communications sent or received by councillor's staff relating to city councillor's city Twitter account
- City of Toronto denied access on basis that it did not have custody or control of the records
- IPC upheld city's decision, found records were personal and political, relating to councillor's activities as elected representative, not under city control

IPC Order MO-4075: Political records – no custody or control

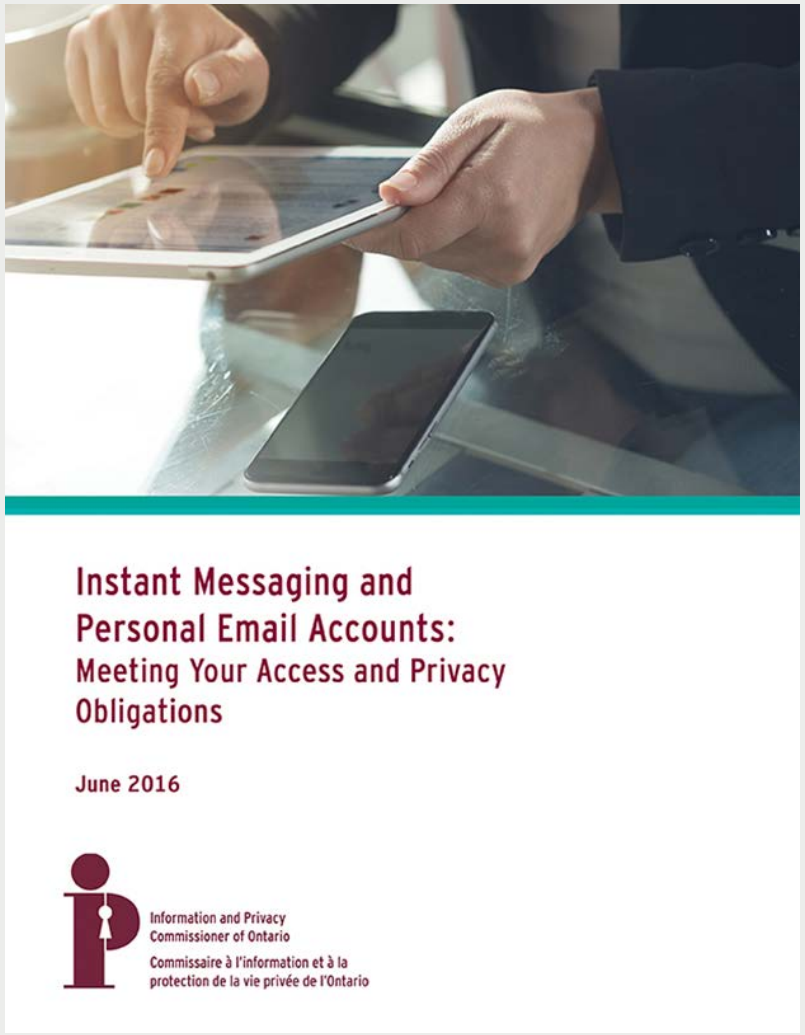
- Access request for correspondence between council members and staff regarding a specified incident, as well as any subsequent discussions between the councillor, his elected and staff colleagues, and third parties about the incident
- Issue on appeal: are the councillor's records in the custody or control of the township?
- IPC found that the councillor's records that were sent or copied to any township officers or employees are in the custody or control of the township
- Councillor's records that were not sent or copied to the township's officers or employees are political records of the councillor and not in the township's custody or control

IPC Order MO-3281: Councillor's emails working on city's behalf – in city's custody or control

- City of Oshawa received a request for access to emails between a councillor and an individual who was retained by the city to investigate alleged wrongdoings of city staff
- The email discussed potential terms of a contract between the city and the individual
- City denied access to the email saying it was not within its custody or control because it was a political or constituency record
- The IPC decided that the councillor was in effect negotiating on behalf of the city; therefore email was in city's control, city then disclosed the emails
- Records related to government business that are sent from a personal email account are subject to access laws

Personal email account and instant messaging

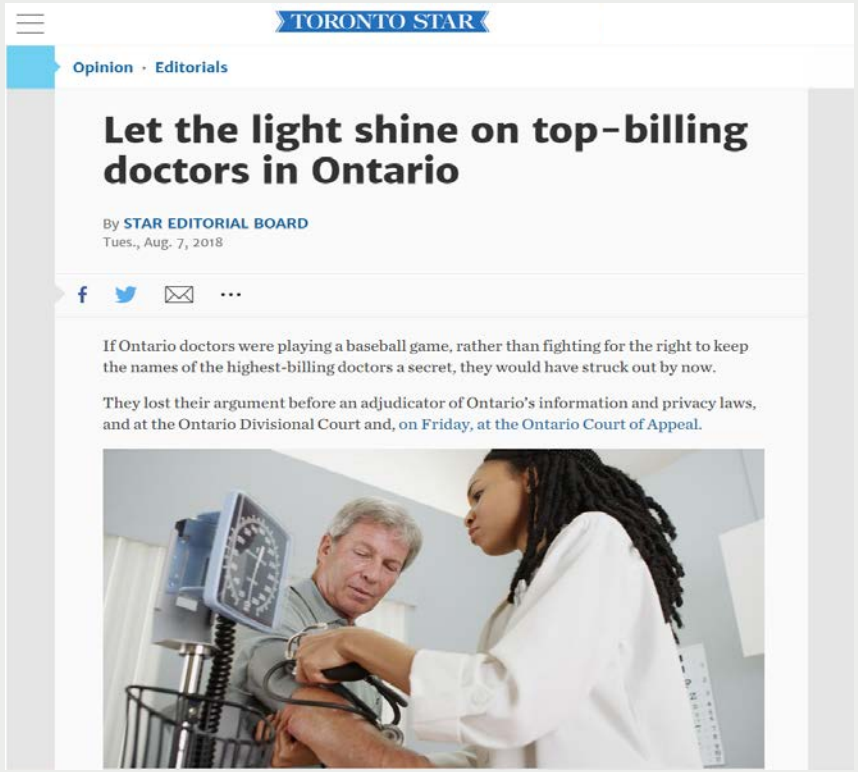
- IPC guidance provides advice on managing these tools in a business environment
- These communications are subject to FOI requests
- A best practice is for institutions to prohibit use, or enact measures to ensure business records are preserved



Hypotheticals and Q&A

OHIP billings

- Toronto Star sought access to top 100 OHIP billing physicians for 2008-2012
- Ministry discloses dollar amounts but withholds names under privacy exemption
- IPC orders disclosure – OHIP billings are "business" not "personal" information
- Decision upheld by the courts on judicial review


TORONTO STAR

Opinion · Editorials

Let the light shine on top-billing doctors in Ontario

By STAR EDITORIAL BOARD
Tues., Aug. 7, 2018

If Ontario doctors were playing a baseball game, rather than fighting for the right to keep the names of the highest-billing doctors a secret, they would have struck out by now.

They lost their argument before an adjudicator of Ontario's information and privacy laws, and at the Ontario Divisional Court and, on Friday, at the Ontario Court of Appeal.

Supreme Court of Canada denies OMA leave

- SCC denies leave to appeal (March 2019)
- IPC's 2016 decision stands
  - sharing names of physicians who bill OHIP with the public falls in line with growing public expectation for transparent government and accountability
  - billings of other professionals and consultants not considered personal information and are accessible to the public under Ontario's access law
  - Ontarians have a right to scrutinize government spending and decision-making; right to access government-held information is a cornerstone of a healthy democracy
  - people need to know what their government is doing to hold it accountable

TORONTO STAR

CANADA POLITICS WORLD OPINION LIFE SPORTS ENTERTAINMENT BUSINESS STA

GTA

They're Ontario's top-billing doctors, but for years their identities have been kept secret. Until now

By May Warren Staff Reporter
Theresa Boyle Health Reporter
Andrew Bailey Data Analyst
Thu., June 27, 2019 | 13 min. read

Mandate letters

- Journalist was refused access to mandate letters to government ministers
- Cabinet Office denied access claiming that "disclosure would reveal the substance of deliberations of the Executive Council or its committees"
- IPC determined that although letters lay out the government's key policy priorities, exemption does not apply because disclosure of the letters would not reveal the substance of any cabinet deliberations, meetings, or discussions
- Government brought an application for judicial review challenging the IPC's order, which the Divisional Court dismissed for number of reasons, including the insufficiency of evidence, and also disagreed that the IPC had erred in interpreting the law
- The government appealed the decision to the Court of Appeal
- The Court heard the appeal on August 31, 2021 and reserved judgement

IPC Order MO-3295: Public interest in information about wrongdoing

- Algoma Public Health (APH) received a request for final report of 2015 KPMG forensic review
- Report relates to whether conflict of interest regarding appointment of APH's former interim CFO, and whether any funds were subsequently misappropriated or lost by APH
- APH decides personal privacy exemption applies, but decides full report should still be disclosed on basis of public interest override
- IPC upholds APH decision to disclose
- April 2019: Ontario Court of Appeal affirms APH/IPC decision

Questions?

Where problems arise

Contentious Issues Management (CIM)

- Some ministries have processes to give ministers a “heads up” about FOI disclosures of potentially controversial records
  - e.g. where requester is from media, opposition party, or sensitive subject matter
- IPC recognizes legitimacy of CIM, if done properly
- Should be for FYI purposes only, not as an approval or “sign-off,” and it must not delay disclosure of records
- “Politically driven influences” on access to information decisions is not acceptable

Report into CIM in the Ministry of Finance

- IPC investigated allegations of political interference in two FOI requests related to actions of a legislative assistant in the office of the Minister of Finance
  - findings: CIM processes, absent politically-driven influences, not inconsistent with government responsibilities under FIPPA
  - no evidence of inappropriate political interference


Sections

thestar.com

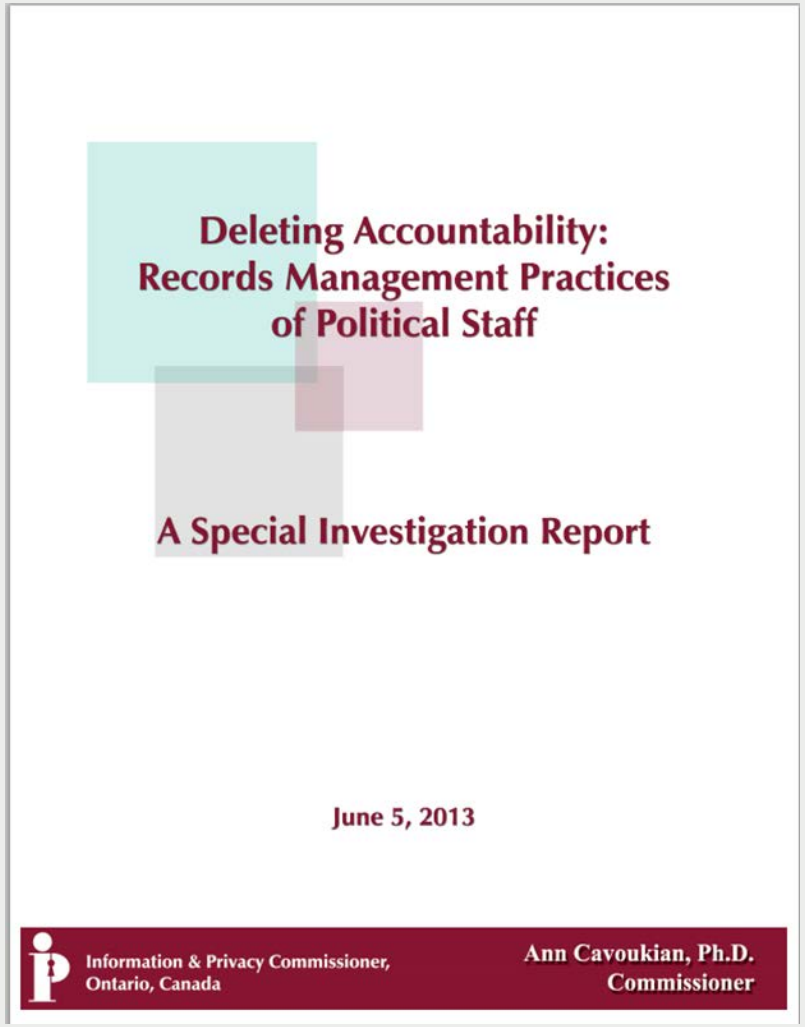
News · Canada

Privacy watchdog clears Ontario finance officials of political meddling

Ontario's privacy watchdog has cleared a finance ministry staffer of allegations of political interference regarding freedom of information requests.

Deleting accountability

- IPC investigated deleted emails relating to the cancellation of gas plants, found that thousands of documents destroyed without authorization
- We made a number of recommendations on appropriate record management practices



Public Sector and MPP Accountability and Transparency Act, 2014

- Effective January 1, 2016
- Institutions must take reasonable measures to preserve records in accordance with existing rules
- Offence to alter, conceal, or destroy record with intention of denying access, $5,000 fine

Protection of privacy

Privacy

- *FIPPA* also protects privacy through rules for the collection, use, and disclosure of personal information by an institution
- No collection unless
  - authorized by statute
  - used for law enforcement
  - necessary to lawfully authorized activity

For example: There must be a legitimate reason for collecting personal information, such as requiring a birth certificate to issue a driver's licence

Privacy obligations under *FIPPA*

No use of personal information unless

- for purpose collected
- for consistent purpose
- with consent

For example: 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 of personal information unless

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

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

Privacy breaches

- Privacy breaches occur when personal information is collected, used, disclosed in ways not authorized by the acts
- Privacy breaches can be:
  - deliberate: police officer looks up ex-girlfriend's information on CPIC
  - 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

Best practices in protecting privacy

- Limit amount of personal information collected and used
- Ask whether 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

Political staff and privacy

- Collection, use, and disclosure of personal information by political parties generally falls outside the scope of *FIPPA*
- However, if political staff were to handle personal information for a purpose related to the administration of a ministry program or service, or in the context of any other ministry related business, *FIPPA*'s privacy rules may apply

Personal Health Information Protection Act (PHIPA)

- Purpose is to protect the confidentiality of personal health information (PHI) in the custody or control of health information custodians and to provide individuals with a right of access to their own PHI and the right to seek correction of such information, with limited exceptions
- *PHIPA* governs PHI in the custody or control of:
  - health information custodian, or
  - agents of health information custodian
- *PHIPA* also contains restrictions on the use and disclosure of PHI by non-health information custodians that receive PHI from health information custodians
- PHI includes any identifying information about an individual's health or health history, health care, payments, eligibility for healthcare, eligibility for coverage for health care, or Ontario health card number

Part X of *Child, Youth and Family Services Act*

- Part X of the *Child, Youth and Family Services Act* (*CYFSA*) contains requirements for records of personal information:
  - collected for or relating to the provision of a service under the *CYFSA*
  - in the custody or control of a service provider
- It applies to:
  - children's aid societies
  - service providers funded under the *CYFSA*
  - all *CYFSA* licensees
- Part X requires consent for the collection, use, and disclosure of personal information, subject to some specific exceptions

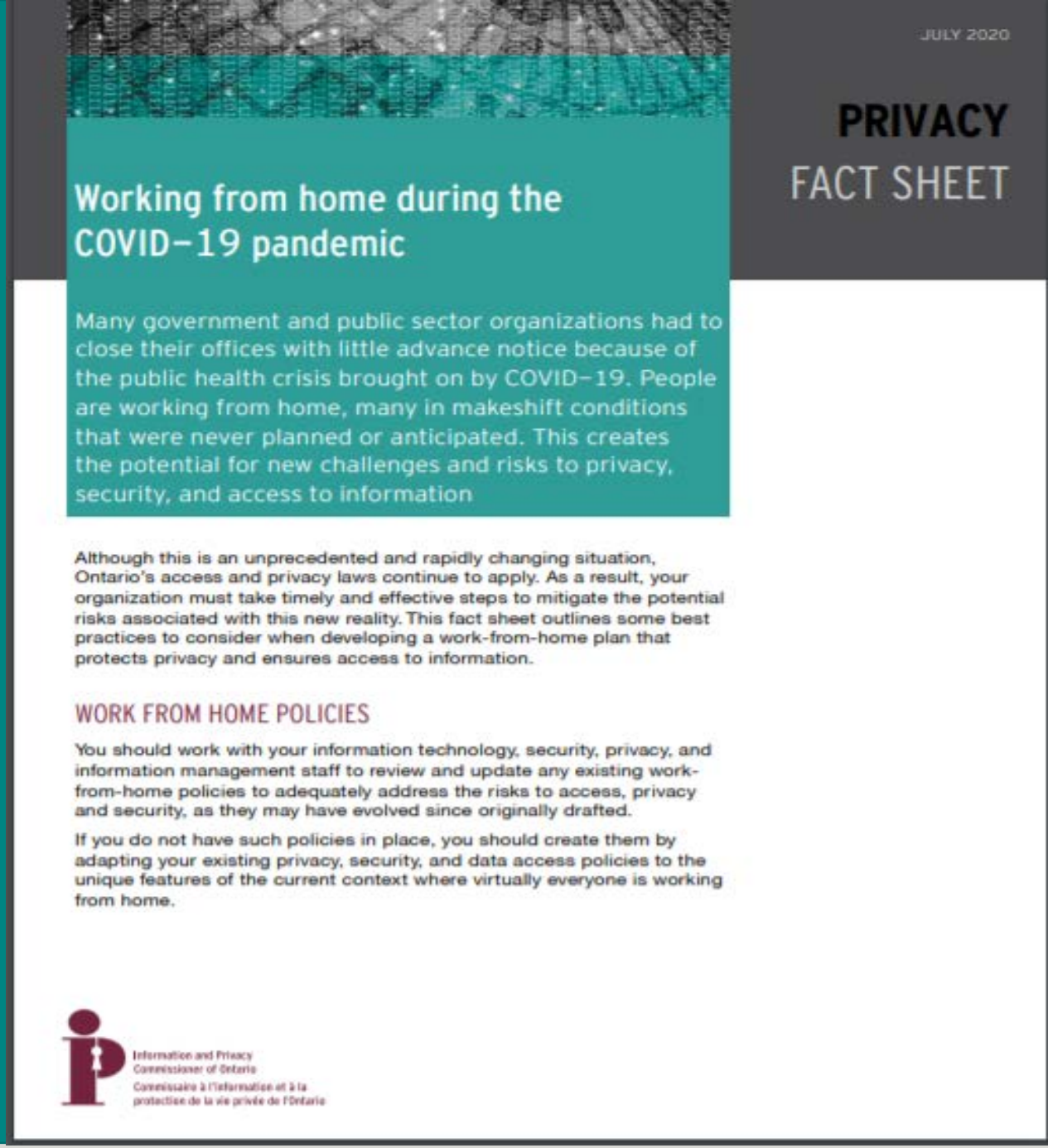
Anti-Racism Act

- Authorizes or requires public sector organizations (PSOs) listed under the regulations to collect and use personal information for the purpose of eliminating systemic racism and advancing racial equity, and sets out privacy obligations to protect that personal information
- Regulation requires PSOs in child welfare, education, and justice sectors to start collecting Indigenous identity, race, religion, and ethnic origin by a defined date in the next five years
- IPC is the oversight body and may:
  - order PSOs to discontinue, change, or implement a practice, and destroy personal information collected
  - comment and make recommendations on privacy implications of any matter related to the act, regulations, or data standards

Working from home

Guides public institutions on home working arrangements during the pandemic

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



JULY 2020

PRIVACY
FACT SHEET

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.

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

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

JULY 2019

TECHNOLOGY FACT SHEET

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

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

Artificial intelligence

The IPC is actively engaged on AI, including a submission to the Ontario *Trustworthy AI Framework* consultation

Privacy, transparency, and other human rights must be addressed throughout AI lifecycle:

- Privacy legislation applies to training data
- Institutions must be transparent regarding AI-powered decision-making
- Individuals must be able to contest automated decisions and the use of AI
- Implement measures to identify, mitigate bias and inaccuracy

Made-in-Ontario Private Sector Privacy Law

Made-in-Ontario private sector privacy law

- August 13, 2020 and July 17, 2021 - Ministry of Government and Consumer Services launched a consultation and white paper to explore whether the time has come for a made-in-Ontario private sector privacy law
- Key areas that the government is considering:
  - increased transparency
  - clear consent provisions
  - right to deletion and de-indexing
  - data portability
  - compliance and enforcement
  - de-identified and derived data
  - expanded scope to include non-commercial organizations
  - data sharing including through data trusts

Ontario's opportunity

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

Questions?

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