

Access and Privacy in Ontario: A Primer

Sherry Liang
Assistant Commissioner

Renee Barrette
Director of Policy

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

Political Staff
Training

February 9, 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.”

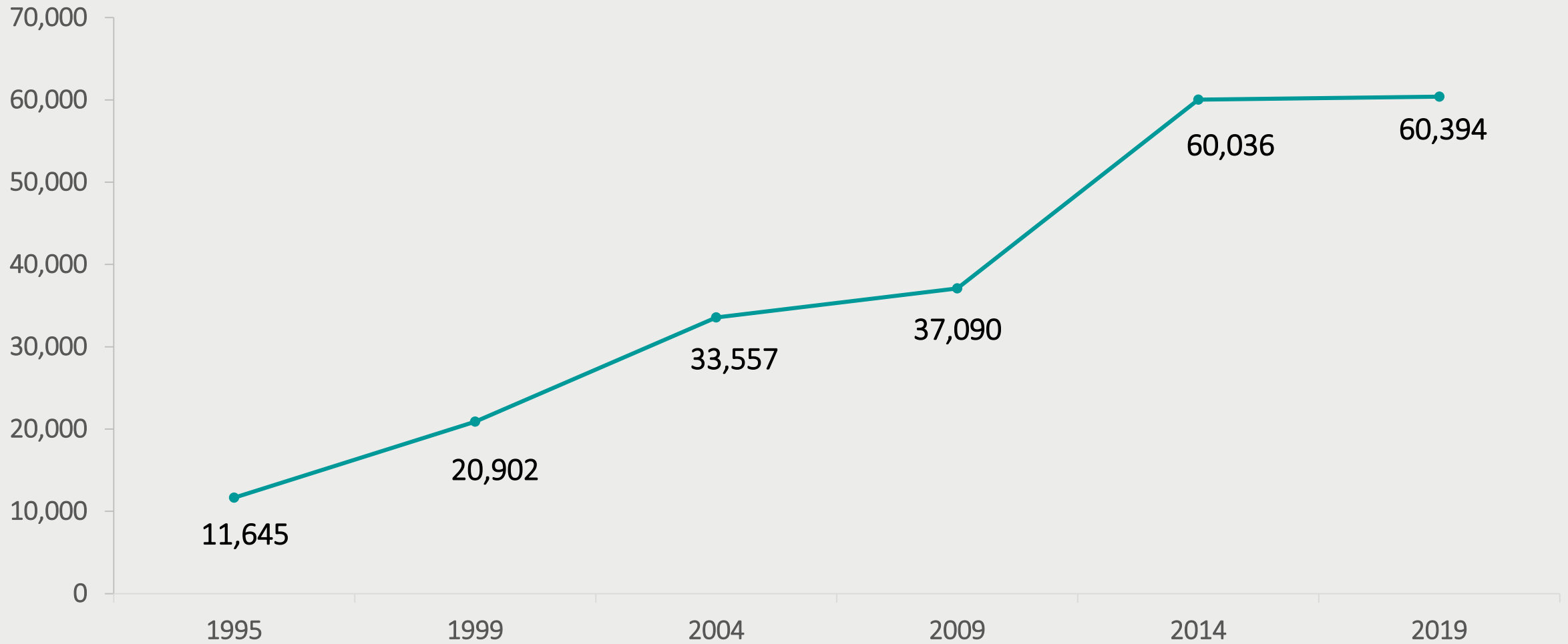
SCC Justice La Forest

Dagg v. Canada (Minister of Finance), 1997

Right of access under *FIPPA/MFIPPA*

- 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 Per Year



Exemptions: Limited and Specific

DISCRETIONARY EXEMPTIONS INCLUDE

- 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)

MANDATORY EXEMPTIONS

- Cabinet records (s.12)
- third party information (s.17)
- someone else's personal information (s.21)

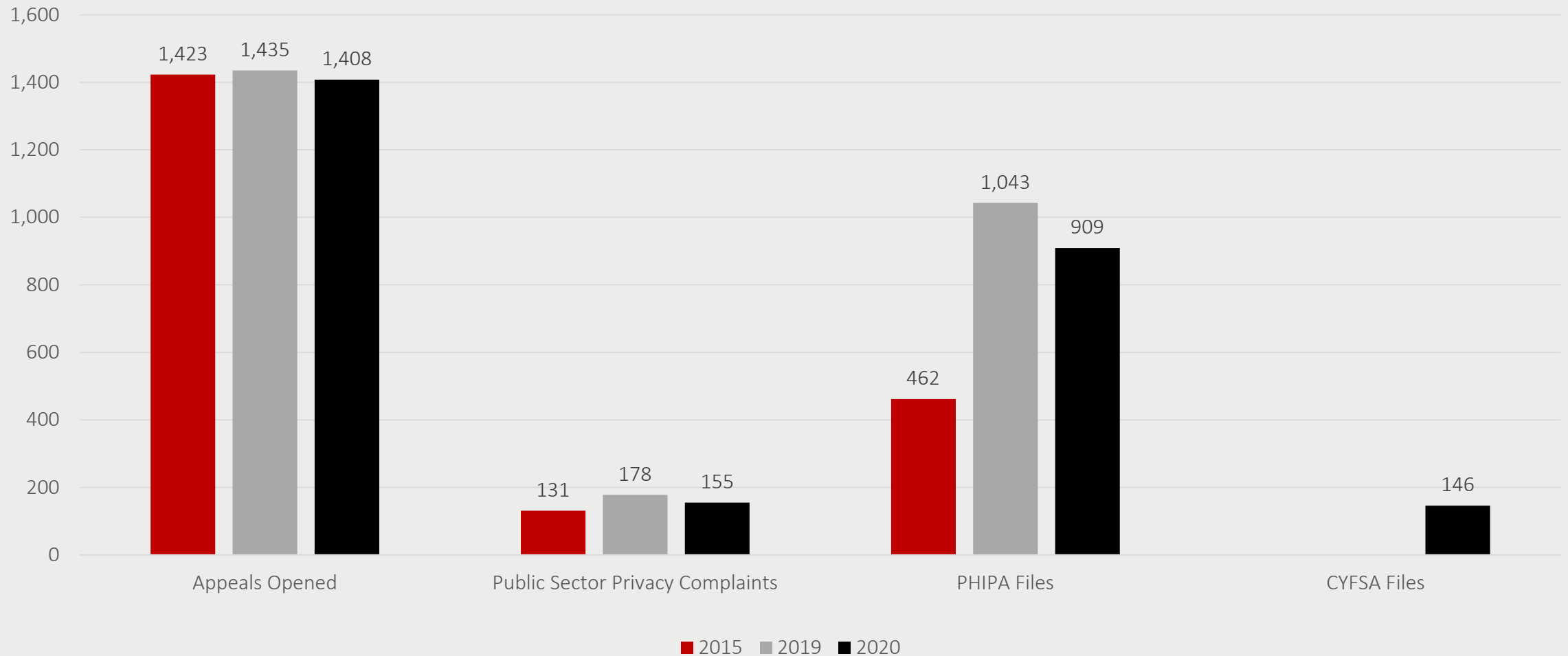
IPC Appeals

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

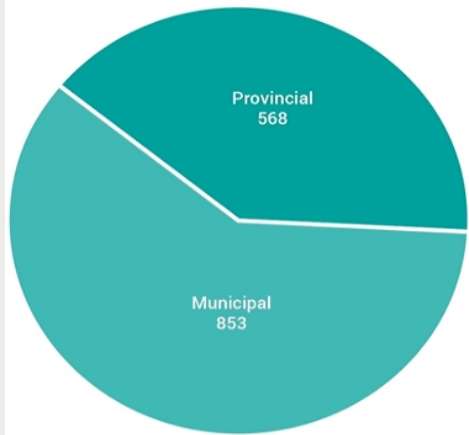
A third party may appeal the institution's decision to disclose information that affects their interests

Appeals, Complaints and Breaches

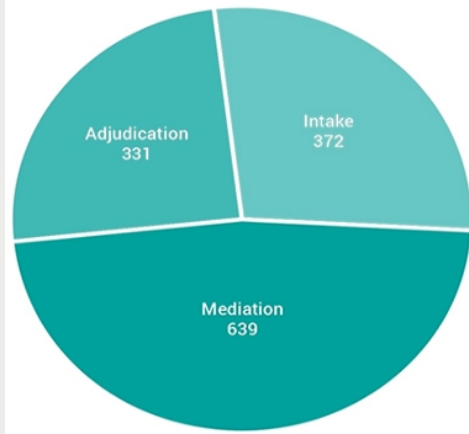


Appeals for 2019

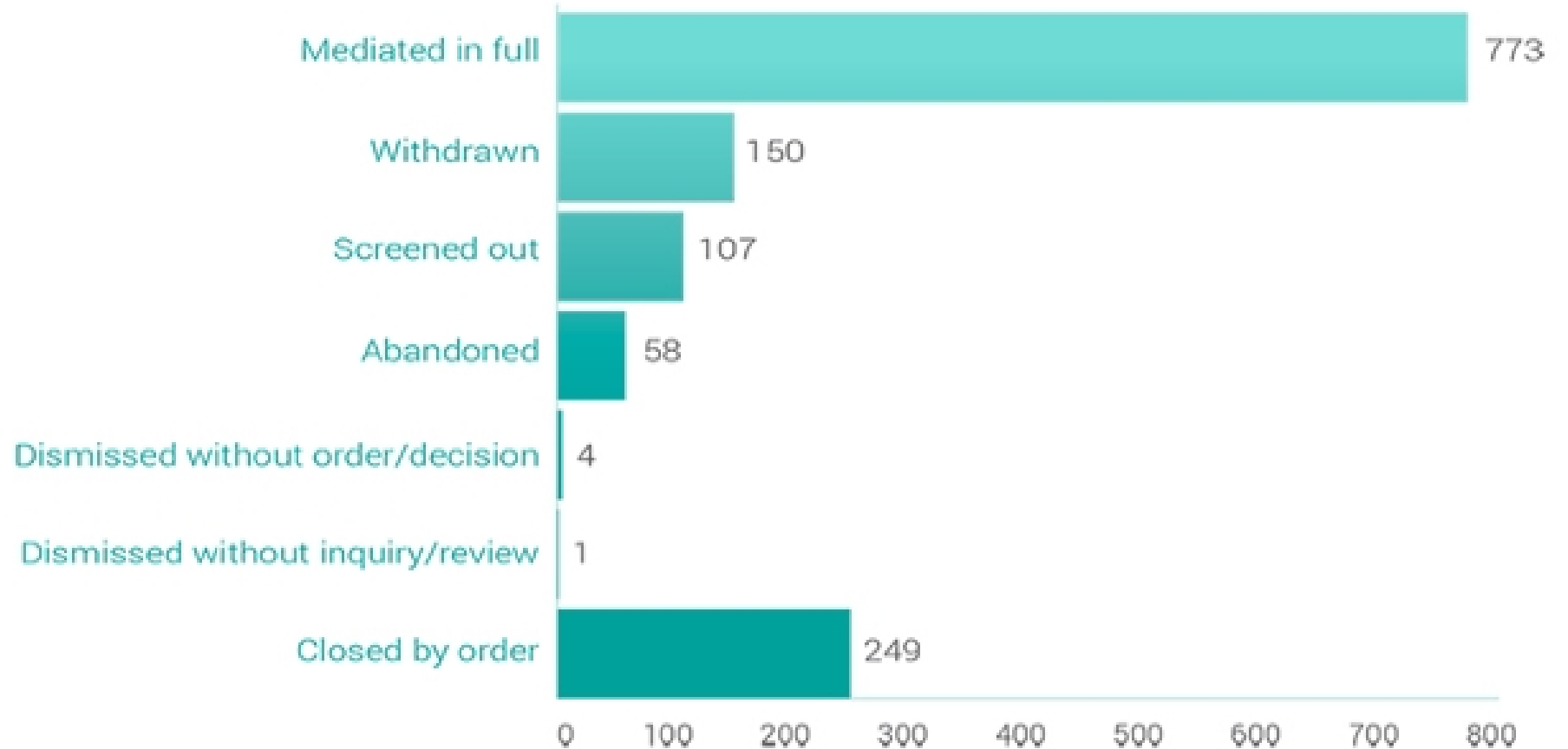
ACCESS APPEALS RECEIVED



APPEALS RESOLVED BY STAGE



OUTCOME OF APPEALS



Political party and constituency records

- Political party/constituency records generally fall **outside the scope of *FIPPA***
- 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/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

- Request for communications sent/received by staff of city councillor concerning councillor's 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

Personal email/instant messaging

IPC Guidance provides advice on managing these tools in a business environment

These communications are subject to FOI requests. Best for institutions to prohibit use, or enact measures to ensure business records are preserved



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

June 2016



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

Premier's mandate letters

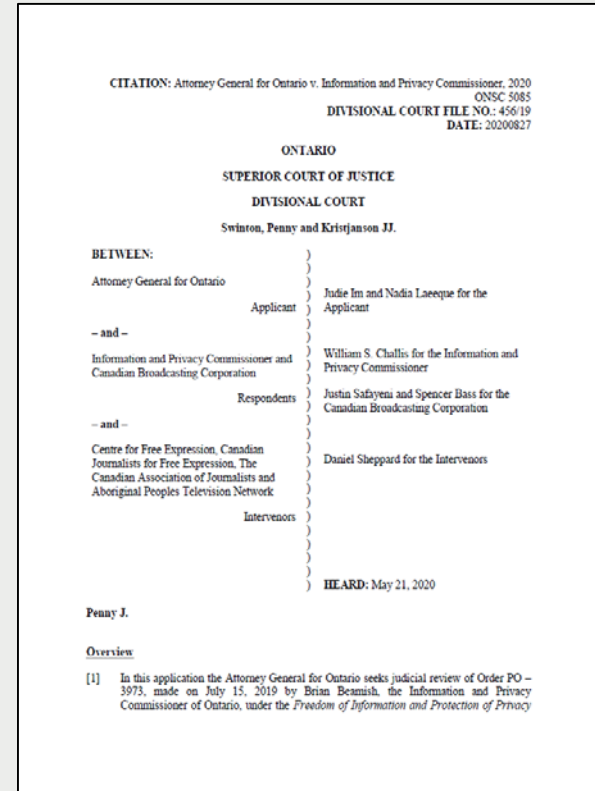
- A requester sought a copy of each of the mandate letters Premier Doug Ford sent to Cabinet Ministers for all of Ontario's ministries, and two non-portfolios.
- The Cabinet Office denied access to all the records claiming the application of the mandatory exemption in s12(1) believing that disclosure would reveal the substance of deliberations of the Executive Council or its committees.
- After reviewing the mandate letters, the adjudicator determined that while the letters laid out the government's key policy priorities, they did not reveal details of any government deliberations, meetings or discussions.
- The government notified the IPC that they intended to challenge the order in court.
- The Divisional Court dismissed an application for judicial review for a number of reasons and also disagreed that the IPC had erred in interpreting the law.

Mandate Letters: Divisional Court

The Court’s characterization of the IPC’s finding in this connection, and its endorsement of this approach, is significant:

“Even assuming, therefore, that the identified policy priorities would be discussed to some degree in some future Cabinet meeting, the IPC found the Letters are articulated at such a high level and in such general terms as to be properly characterized as “subject matters” and “topics” for future deliberation, not disclosure of any deliberations themselves. ... I can find no basis to conclude that the IPC acted unreasonably in reaching its conclusion.”

— Ontario Superior Court of Justice Divisional Court, Swinton, Penny and Kristjanson JJ., May 21, 2020.



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”
- Ontario Medical Association seeks review at Ontario Divisional Court – dismissed
- OMA appeals – Court of Appeal upholds IPC
An individual's gross professional or business income is not a reliable indicator of the individual's actual personal finances or income [not PI]

TORONTO STAR

News · GTA

Appeal court ends secrecy of payments to Ontario's top-billing doctors

By **THERESA BOYLE** Health Reporter
Fri., Aug. 3, 2018

TORONTO STAR

Opinion · Editorials


Let the light shine on top-billing doctors in Ontario

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

f t e ...

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 legislation
 - Ontarians have a right to **scrutinize government spending and decision-making**; right to access government-held information is a cornerstone of a healthy democracy
 - individuals need to know what their government is doing to hold it accountable



Algoma Health – public interest in information about wrongdoing

- **Order MO-3295** – request to Algoma Public Health for KPMG forensic report
- Report on whether **conflict of interest** in appointment of CFO, whether any funds misappropriated/lost
- 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
- Ontario Court of Appeal affirms APH/IPC decision (April 2019)



Where problems arise

Contentious Issues Management (CIM)

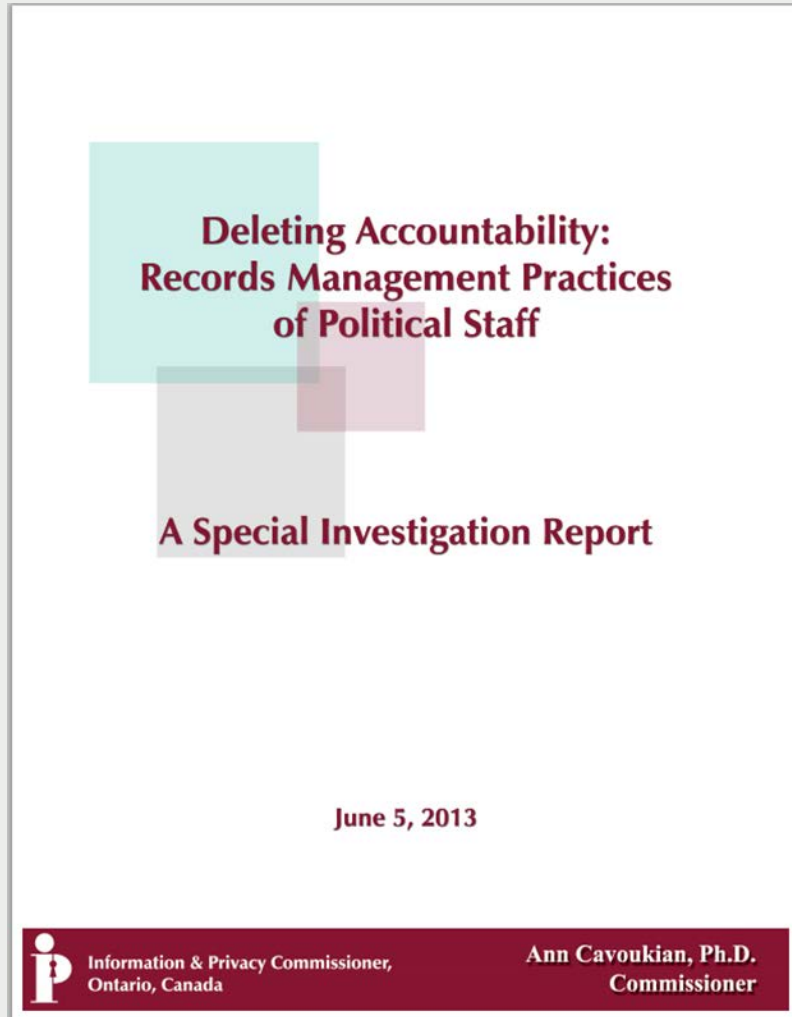
- Some ministries have processes to give ministers a “heads up” about FOI disclosures of potentially controversial records
 - e.g. where requester is from **media, opposition party, or sensitive** subject matter
- IPC recognizes legitimacy of CIM, if done properly
- Should be for **FYI purposes only**,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

Deleting Accountability



- IPC investigated **deleted emails** relating to 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, destroy record with intention of denying access, \$5,000 fine



Protection of Privacy

Privacy

FIPPA also 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 *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

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

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

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



Made-in-Ontario Private Sector Privacy Law

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
- Key areas that the government is considering:
 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

Access and privacy rules for political parties

A hand in a blue shirt sleeve is shown dropping a white ballot into a grey ballot box. The background is dark, and the scene is lit from the side, creating a dramatic effect.

- Political parties collect large volumes of sensitive personal information to target voters
- Increasingly sophisticated tools raise new privacy and ethical concerns – see Cambridge Analytica
- Resolution passed by cross-Canada Commissioners in 2018 calling for action
- Federal *Election Modernization Act*, 2018
- February 2019 Élections Québec report recommending protection of personal information held by political parties... enter Bill 64



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

E-mail: info@ipc.on.ca

Media: media@ipc.on.ca / 416-326-3965