Third-Party Educational Apps and the Importance of Adequate Privacy Training

Warren Mar, Assistant Commissioner
Lucy Costa, Manager of Investigations

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

TDSB – IPC Presentation

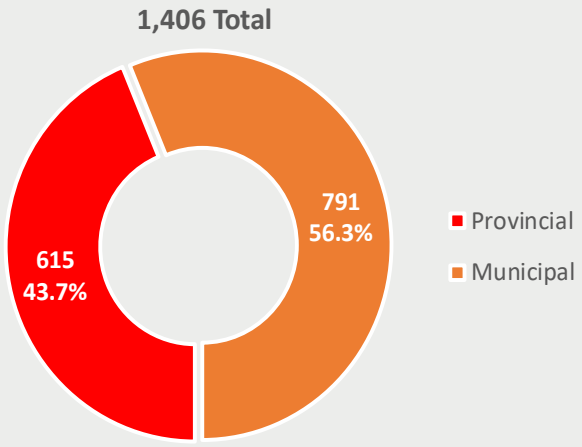
November 28, 2022

1. Tribunal Operations

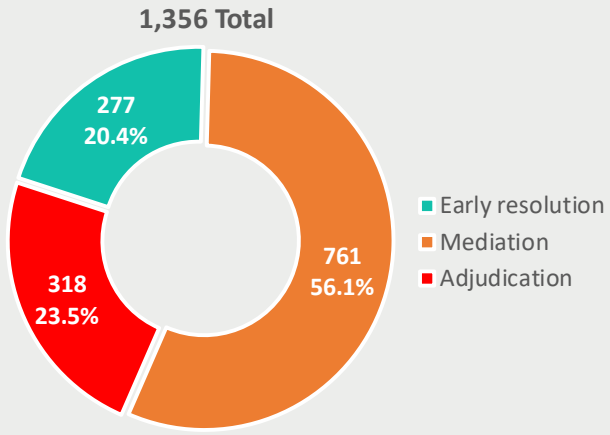
Tribunal Info

- 2021 Stats for FIPPA/MFIPPA Appeals:

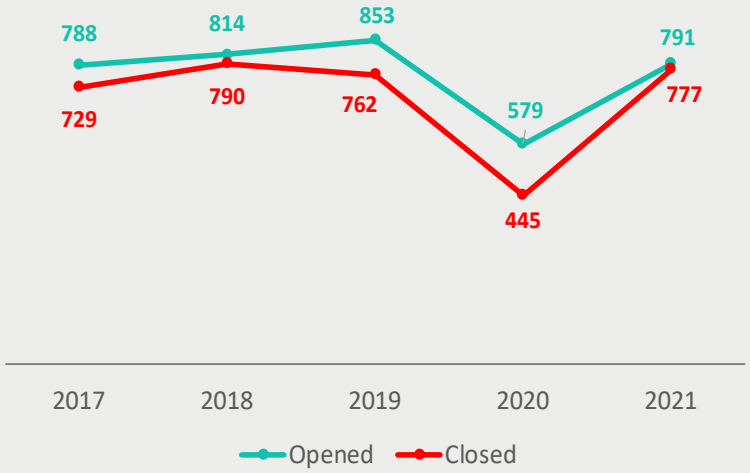
Access Appeals Opened



Access Appeals Resolved – By Stage



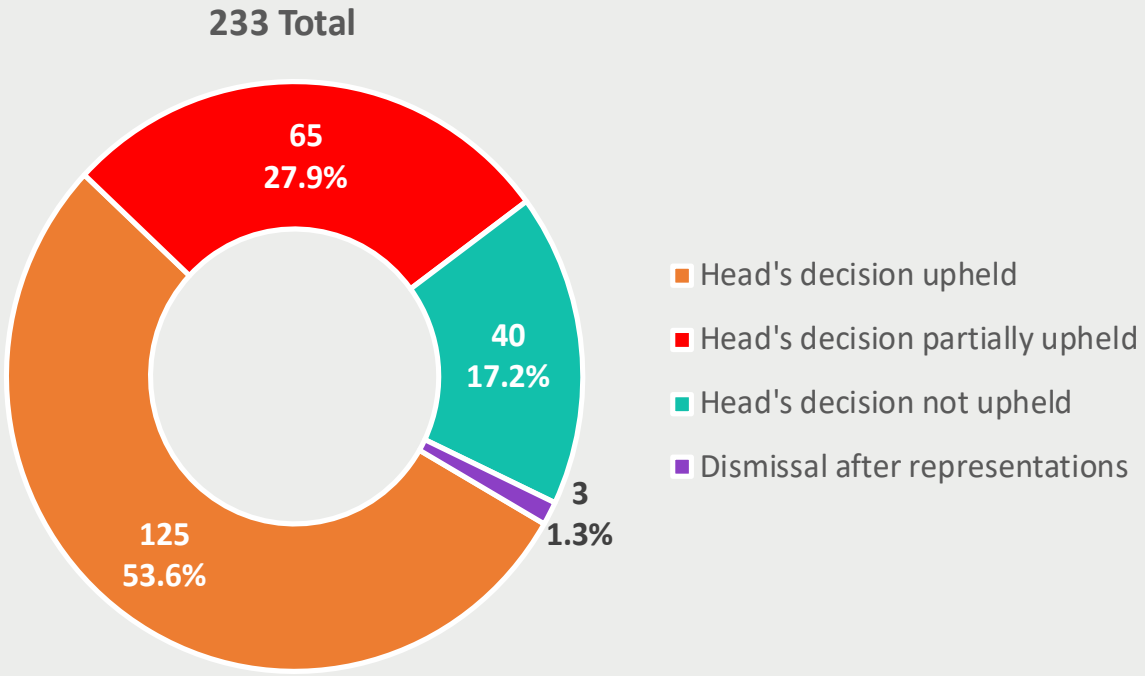
MFIPPA Appeals Opened/Closed 2017 – 2021



Cont'd

Tribunal Info

- 2021 statistics – outcome of FIPPA/MFIPPA appeals closed by order*:



** Does not include files that were resolved, abandoned, withdrawn, or dismissed without an inquiry during adjudication.*

Cont'd

Tribunal Info

- Increase in privacy complaints, and institutions self-reporting data breaches involving sophisticated forms of ransomware and cyberattacks + increasing demands on the Tribunal:
  - **28% increase** in processing time for files (from 7.1 months to close a file in 2017 to 9.9 months in 2021)
  - **65% increase** in cyberattack / ransomware files in the last 5 years (from 590 files to 971 files)
  - **78% increase** in privacy breaches reported to the IPC from 2017 to 2021 (from 439 files to 783 files)
- Investigations have become more complex and they take longer to resolve, given the complicated technological and legal issues involved.

Impact of COVID-19 on the IPC

- Prior to the pandemic, the IPC's processes were heavily paper-based – moved to virtual model & electronic documents.
- The IPC Policy Division is busy providing advice to government and broader public sector institutions as they deal with COVID-19: accelerated digitization, e-learning, and the use and sharing of data.
- No reduction or suspension in the statutory timeframes to process access requests or file appeals – unlike other government services or other judicial/quasi-judicial sectors.

IPC Tribunal Lean Process Review

- Examine and improve the **processes** that individuals and institutions interact with on a regular basis to better manage caseload and improve service.
- Create a “best-in-class” Tribunal that is fair, timely, and meaningful to Ontarians.
- Developing a culture of continuous improvement and empowerment to:
  - utilize our budget in a way that provides the most value;
  - improve the quality of our operations;
  - process files, and issue decisions and reports, more quickly; and
  - increase our responsiveness with institutions and the public.

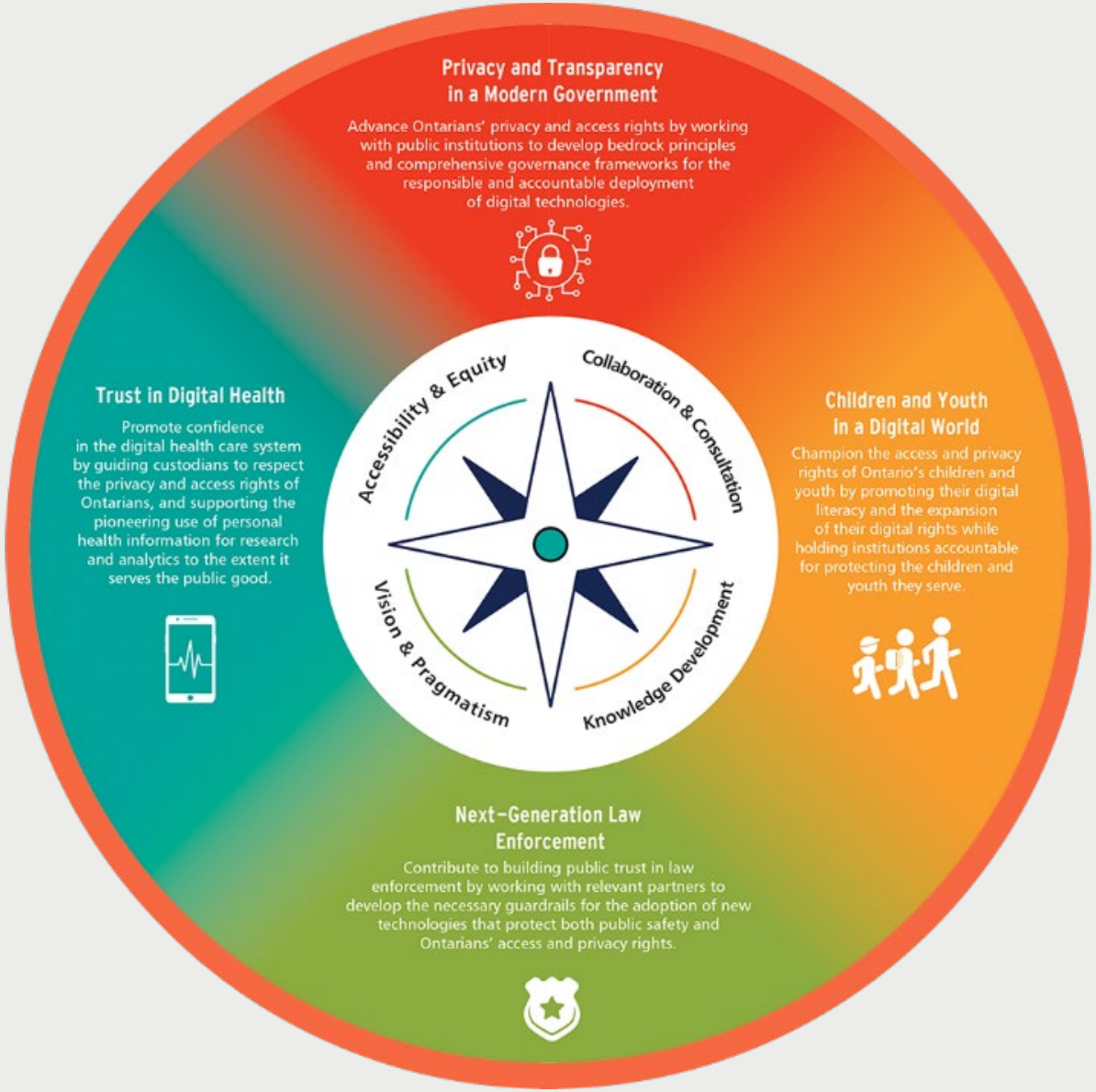
Moving to Online Services

- We have **implemented a ShareFile system to** allow institutions to submit records to us electronically, via a secure platform.
- In August 2022, the IPC launched **two new online services** that streamline the appeal process and improve accessibility:
  - an **electronic appeal form** that can be submitted online; and
  - a **secure payment portal** that enables the public to submit their appeal and required fee online.
- Paper appeal forms and cheques will still be accepted; fees remain the same.

2. Third-Party Apps and Online Educational Tools – Protecting Students' Privacy

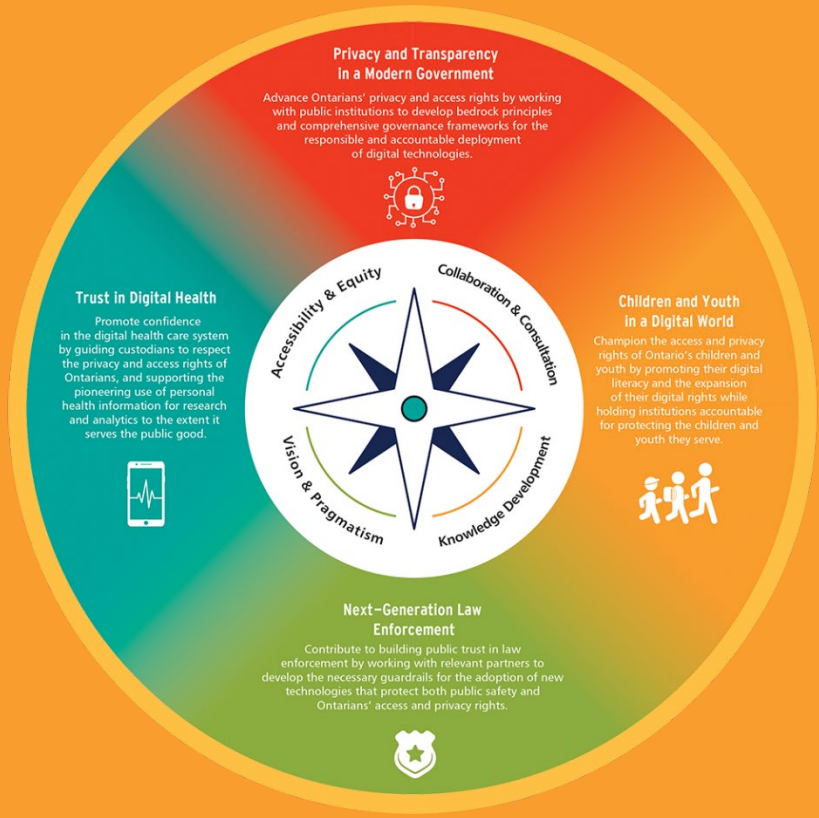
IPC's Strategic Priorities

- Privacy and Transparency in a Modern Government
- Children and Youth in a Digital World
- Next-generation Law Enforcement
- Trust in Digital Health



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.

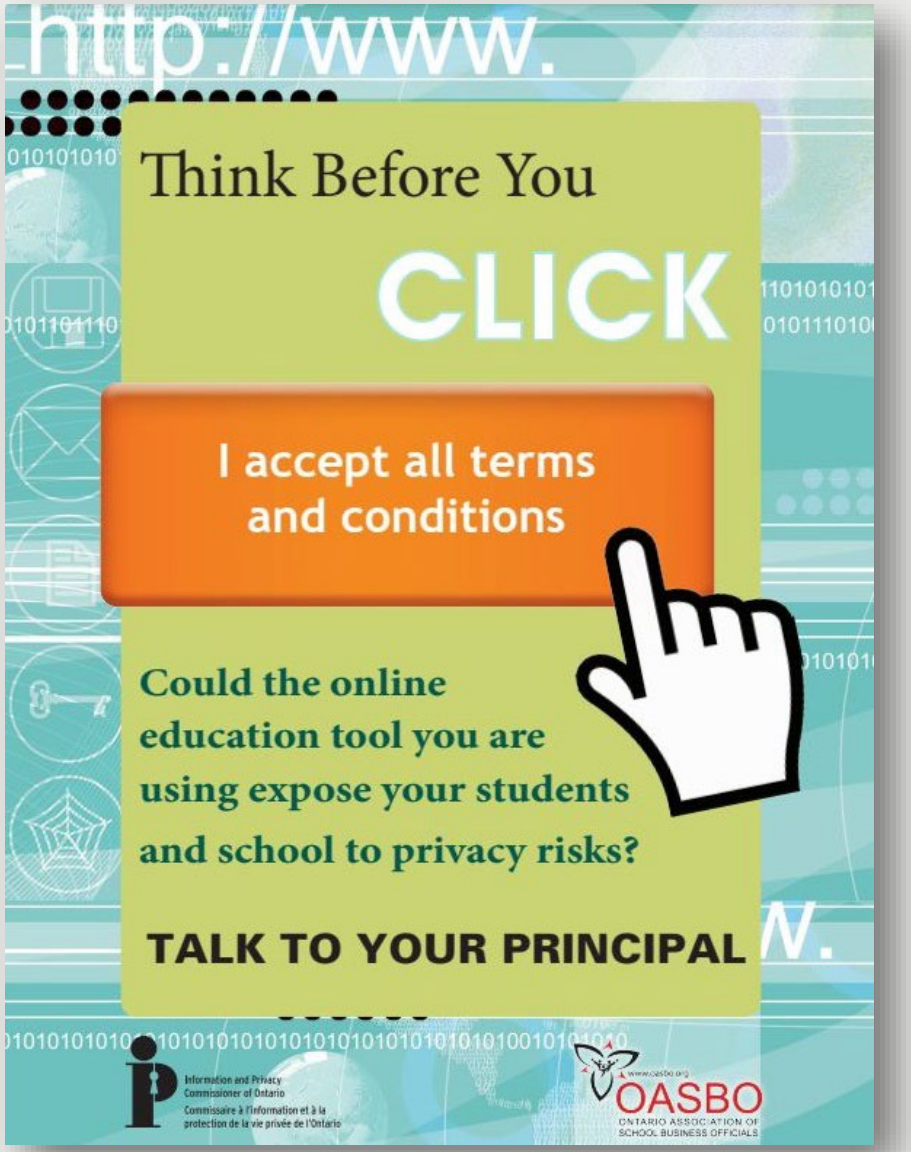


IPC Interest in Educational Technologies

- Classroom management and learning apps
- Video conferencing platforms
- Remote proctoring
- Student monitoring and surveillance
- Cloud computing and other third-party platforms
- Breaches of privacy and security

Use of Online Educational Services

- School boards are accountable
- Caution when collecting, using or disclosing students' personal information online
- Some online educational tools and services:
  - collect personal information of students for non-educational purposes
  - track students' online activities outside of school
  - use students' behaviour and performance to target market products or services
  - disclose personal information to other parties



Use of Online Educational Services

Best practices for school boards

- Policies to evaluate, approve online educational services
- Ensure staff and educators use only approved services
- Privacy and security training, ongoing support
- Notices of collection
- Opt-out (where feasible)
- Retention periods

Protecting Students' Privacy Online

Teachers considering the use of online educational tools and services should:

- **Consult** with school officials
- Read and understand privacy policies and **terms of service**
- Use only apps and services **approved** by the school board and Ministry of Education
- Provide students with **guidance on use**
- Use services that **minimize** collection, use and disclosure of identifiable information

JANUARY 2019

EDUCATION
FACT SHEET

Protecting Your Students' Privacy Online

Online educational tools and social media provide new opportunities for teachers to learn, enhance educational techniques and connect with students, parents, and the greater community. Protecting students' privacy in the age of technology has never been more important.

PRIVACY RISKS OF ONLINE TOOLS AND SERVICES

Terms and conditions and privacy policies for online tools can make it difficult to determine if you are complying with provincial privacy laws. For example, some online services:

- collect and retain students' and parents' personal information such as names and email addresses
- track and record online activities and interactions with other students
- evaluate students' performance to generate learning profiles and market products directly to students and parents
- sell students' information to third parties

The Information and Privacy Commissioner of Ontario recommends that teachers considering the use of online educational services:

- consult with school officials before selecting these services
- read privacy policies and terms of service carefully to understand how students' information may be collected, used and disclosed
- only use school board approved apps and services

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

MC18-48: York Region District School Board

- Complaint over YRDSB using cloud-based storage and data management service provider to manage attendance matters.
- Parents felt it was a big change from the old system, that they didn't consent to or expect it to happen.
- Nothing in the *Act* prevented the board from moving to a new way of doing this.
- Clear that attendance was included among educational services, and that board (and its agent) could collect and use student information for that purpose.

MC17-52: Toronto District School Board

- Parent objected to student using Google Workspace for Education core services; concerned about:
  - failure to notify parents, and obtain consent to collect, use, and disclose students' personal information
  - use of personal information beyond scope permitted under MFIPPA
  - storage of personal information outside of Canada
  - inadequate security protections
  - lack of adequate data deletion and retention practices
- Board was using a version that had been negotiated for by the Ministry of Education, with additional restrictions.
- Included an addendum that student information could only be used by Google to provide these core services.
- Student information was collected for the purpose of providing educational services, and these restrictions limited the use to those purposes.

MC18-17: Halton District School Board

- Parents stated that board failed to have a system in place to restrict the use of apps in Google Marketplace or provide guidance on their use.
- During investigation, HDSB put in place a “stoplight” system that they used to categorize apps:
  - Green – use without concern
  - Yellow – use with caution, following guidance in place
  - Red – do not use (not available for use or download)
- Vendors accessing personal information must enter into usage agreements with board.

MC18-17: Halton District School Board

- Collection Test (section 28(1) of MFIPPA):
  - No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement **or necessary to the proper administration of a lawfully authorized activity.**
- Two-part question:
  - Were the apps necessary?
  - Did the apps only collect the information the vendors needed to provide the services?

Cont'd

MC18-17: Halton District School Board

- Use of personal information:
  - Section 31(b): An institution shall not use personal information in its custody or under its control except… for the purpose for which it was obtained or compiled or for a consistent purpose;
  - Section 33: The purpose of a use or disclosure of personal information that has been collected directly from the individual to whom the information relates is a consistent purpose under clauses 31(b) and 32(c) **only if the individual might reasonably have expected such a use or disclosure**.

Cont'd

MC18-17: Halton District School Board

- Usage Agreement Restrictions:

  5. The Vendor agrees that the Personal Information of students and/or parents/guardians [or employees] may only be collected, used, retained and disclosed by the Vendor **for the purpose of fulfilling its contractual obligations to the Board**.

  6. The Vendor agrees that any Personal Information collected, used, retained and/or disclosed by the Vendor during the course of providing goods/services for the Board shall remain under the control and direction of the Board for the sole purpose of providing goods/services for the Board and for no other purpose. **The Vendor shall not collect, access, use, retain, disclose, sell or share Personal Information for its own benefit or purpose.**

Cont'd

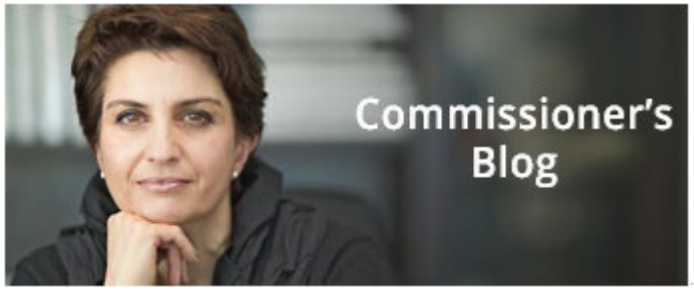
MC18-17: Halton District School Board

- Use for Marketing or Advertising:
  - For a use to be for a consistent purpose consistent with the purpose of its collection, there needs to be a **rational connection** between the two
  - No such connection between collecting information to provide educational services and then using that information to market third party products or services

Cont'd

MC18-17: Halton District School Board

- Expectation of Privacy (Para. 125):
  - Students have a reasonable expectation of privacy in the personal information they provide access to in the course of receiving their education. Students, parents, and guardians must rely on the board's expertise to determine the apps that students require for their education. It is reasonable for them to expect the board put in place safeguards to ensure that the information is used only for those purposes.



www.ipc.on.ca/media-centre/blog/

Back to school: Lessons learned about online educational tools and platforms

Sep 09 2021

Last fall, when the COVID-19 pandemic steered students away from schools and into their homes, school boards and schools needed to pivot on a dime and be certain that the online tools and data management systems they adopted kept students' personal information safe and secure. Following a long shutdown, public schools across the province have welcomed students back into the classroom, but many of the online educational tools are here to stay.

Ontario's municipal privacy law, *MFIPPA*, requires that public school boards and schools ensure that online tools and data management systems properly protect students' personal information. Despite this, it is not unusual for my office to hear from concerned parents and guardians about the adequacy of the privacy and security measures used by their kids' schools.

To help schools navigate this tricky terrain and support compliance, my office has posted a new **webinar** for teachers and school administrators on their access and privacy obligations under *MFIPPA*. It offers a refresher on *MFIPPA* requirements and includes details about recent investigations by my office related to the use of cloud-based data management systems by two of the largest public school boards in the province.

Both these investigation reports bring to light the responsibility of institutions to maintain strong oversight over their service providers and to ensure the personal information they transfer to their service provider for processing is managed in accordance with Ontario's privacy laws.

The York District School Board (YDSB) **investigation** involves the use of Edsby, a cloud-based data management service that stores and processes student attendance information. Our investigation found that while the YDSB had included appropriate provisions in its contract with CoreFour Inc. (Edsby's parent company), it did not have reasonable oversight measures in place to ensure fulfillment of the contract and prevent security vulnerabilities. To address this, our report recommends the school board strengthen and document the steps they have taken to ensure CoreFour has fulfilled the mandatory security requirements of their agreement. This includes, among other measures, confirming the company has implemented the recommendations made in an independent security assessment and having information security policies and controls that align with recognized standards.

Holding Institutions Accountable

- IPC concluded three privacy complaint investigations involving Ontario school boards' use of online educational services.
- Each investigation differed in important ways, but all involved:
  - procurement and use of cloud-based services of third-party private-sector service providers acting as agents
  - direct access and use by students of online, account-based services
  - parent concerns about improper collection, use and disclosure of students' personal information

Cont'd

Holding Institutions Accountable

- IPC investigators found school boards broadly in compliance with MFIPPA, but made recommendations to address some deficiencies, notably to:
  - improve transparency of information management practices, including enhanced notices of collection
  - establish clear privacy and security requirements, consistent with MFIPPA obligations, when contracting online educational services
  - ensuring privacy and security requirements in contracts are kept up to date, and enforced

Takeaways

- IPC privacy complaint reports:
  - provide guidance to school boards, who retain technology service providers to help deliver their education mandates, on the types of contractual provisions they should seek to include in their contracts
  - serve as a reminder that, to fulfil privacy and security obligations, boards must couple a strong contract with appropriate monitoring and oversight

3. The Importance of Privacy Training

Robust Privacy Training

- Ongoing need for institutions, including school boards, to have and maintain their privacy policies and processes.
- Equally important to properly communicate them to staff through regular, ongoing training and other means – especially as technology advances.
- A number of files in the Tribunal have illustrated how proper training could have prevented privacy complaints or mitigated the impact of privacy breaches.

Privacy Complaint Report MC18-39

- A supply teacher video recorded two students on the playground without consent.
- The school board and the IPC's investigation determined the video contained the personal information of the students, and the collection was contrary to the *Act.*
- The investigation also identified a gap in the training and communication to supply staff about privacy.

Cont'd

Privacy Complaint Report MC18-39

- As part of the remediation, the school board:
  - Undertook a review of staff training
  - Drafted new confidentiality agreements for all employees to sign with respect to the new security measures
  - Incorporated training on the *Act*'s privacy protection provisions for supply teachers
  - Sent a communication to staff reminding them of the appropriate use of personal electronic devices

Privacy Complaint Report PC18-00074

- Allegation that an OPP officer accessed the personal information of a civilian and disclosed it to the civilian's husband.
- Investigation by the Professional Standards Bureau concluded the officer had accessed an incident report regarding the civilian on two occasions.
- The officer admitted to accessing the reports out of curiosity.
- The accesses were found not to be in accordance with the *Act*.

Cont'd

Privacy Complaint Report PC18-00074

- IPC's investigation discovered that:
  - The OPP was not providing annual privacy training
  - The IPC investigator also took the view that based on the lack of communication about privacy, the officer may not have been aware this was a breach
- IPC's recommendations included:
  - Enhance/revise documents to clearly communicate that staff are not permitted to access personal information for reasons unrelated to their work
  - Review current training program to ensure that it provides adequate and specific privacy protection against unauthorized accesses to sensitive personal information

Privacy Complaint Report MC19-00058/ MC19-00059

- Allegation that a Toronto Police Service employee was accessing the personal information of tenants in her building (by accessing the police database).
- Audits confirmed (and the investigation found) that the accesses had occurred and that they were not in accordance with the *Act.*
- The Toronto Police could not confirm when the employee had received privacy training and declined to provide this office with their training material.

Privacy Complaint Report MC19-00058/ MC19-00059

Cont'd

- The investigator found, among other things, that the Toronto Police Service did not have reasonable measures in place to prevent unauthorized access of personal information.
- The Privacy Complaint Report's recommendations included:
  - Enhancing their guidance documents to clearly communicate to staff about accesses and uses of personal information in the police database
  - Reviewing its current privacy training program and revise it as necessary to ensure that it provides adequate and specific privacy training against unauthorized accesses to personal information in its databases

Decision 174

- Involved two breach reports submitted by a hospital to the IPC.
- The first involved a nurse inappropriately accessing her own personal health records and that of patients.
- The second involved a clerk at a hospital who accessed a patient's personal health information and posted it on Facebook.

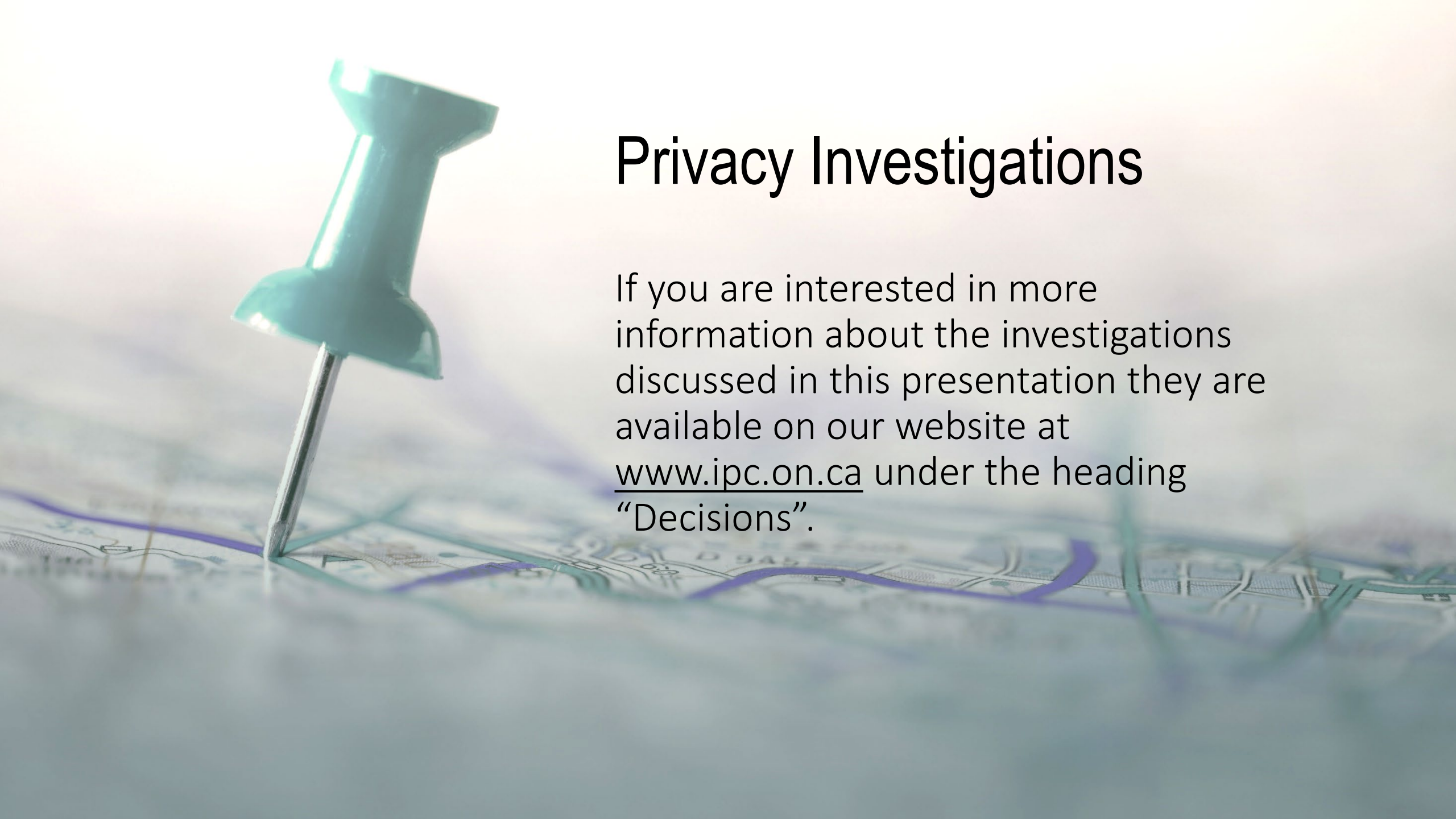
Cont'd

Decision 174

- The hospital investigated and reported these matters to the IPC as breaches.
- The IPC reviewed the hospital's privacy policies and training and found that:
  - There were gaps in the privacy training
  - It was not clear that hospital employees were being given sufficient reminders of their privacy obligations
  - The hospital failed to adequately inform the nurse when she was allowed to access personal health information

Decision 174

- The hospital's remedial action included:
  - Providing increased privacy training, and documenting that the training has been provided
  - Providing annual privacy training that clearly communicates employees' privacy obligations in an understandable way
  - Privacy reminders are sent throughout the year
  - Employees are reminded of their privacy obligations each time they log into the patient electronic record
- The IPC was satisfied that the hospital addressed the gaps identified in the investigation.



Privacy Investigations

If you are interested in more information about the investigations discussed in this presentation they are available on our website at www.ipc.on.ca under the heading "Decisions".

Resources

- IPC Practices: *Drafting a Letter Refusing Access to a Record*

https://www.ipc.on.ca/wp-content/uploads/Resources/num-1.pdf

- Fact Sheet: *Frivolous and Vexatious Requests*

https://www.ipc.on.ca/wp-content/uploads/2017/08/fs-access-friv-vex.pdf

- Fact Sheet: *Labour Relations and Employment Exclusion*

https://www.ipc.on.ca/wp-content/uploads/2020/06/labour-relations-employment-exclusion.pdf

- Fact Sheet: *Public Interest Disclosure*

https://www.ipc.on.ca/wp-content/uploads/2021/09/fs-access-public-interest-disclosure.pdf

- Fact Sheet: *Reasonable search*

https://www.ipc.on.ca/wp-content/uploads/2017/04/fs-access-reasonable-search.pdf

- Fact Sheet: *Third Party Information Exemption*

https://www.ipc.on.ca/wp-content/uploads/2018/09/fs-access-third-party-info-exemption.pdf

- Protocol: *Solicitor-Client Privilege*

https://www.ipc.on.ca/wp-content/uploads/2020/06/2020-06-19-ipc-protocol-cases-involving-privilege-claims.pdf

- Search IPC Decisions:

https://decisions.ipc.on.ca/ipc-cipvp/en/nav.do

THANK YOU!

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