

# Update from the New Commissioner

Patricia Kosseim

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

Ontario  
Connections

October 21, 2020

# Some Early Directions

- Focus on issues that matter most to Ontarians, informed by the broader global policy context
- Collaborate with Canadian and international counterparts on cross-jurisdictional matters
- Take a fair, practical and balanced approach to interpreting and applying new statutory provisions
  - new administrative penalties under *PHIPA*
  - data integration units under *FIPPA*
  - privacy protections in *Part X* of *CYFSA*
- Continue to build on IPC's strong legacy of public outreach and education
- Connect with as many Ontarians as possible, y compris les Franco-Ontariennes et les Franco-Ontariens

# What's Further Down the Road

- IPC Strategic Access and Privacy Priorities (Five-Year Plan)
- Objective is to focus efforts and allocate limited resources to key issues that are of greatest importance to Ontarians, and on which the IPC is most likely to have positive impact.
- Seeking assistance of an Ad Hoc External Advisory Board
- Will be holding an open stakeholder / public consultation process
- Launch of new Strategic Priorities planned for early 2021



**No exposure detected**

# COVID Alert App

- IPC and OPC support use of exposure notification app, conditional on its continued voluntariness and ongoing evaluation for effectiveness
- Worked closely with the Ontario government, and in collaboration with Federal Office of the Privacy Commissioner who worked closely with Health Canada
- Detailed review of the Ontario PIA and Federal-Ontario MOU based on F/P/T Joint Privacy principles for contact tracing and similar apps
- All IPC recommendations were adopted
- Government of Ontario continues to be subject to Ontario's privacy laws
- IPC continuing oversight to review any changes to the app that may affect its security safeguards and ensure that the app be decommissioned if it is no longer achieving its purpose.

# 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

# FAQs re Impacts of COVID-19 on FOIP operations

## Deemed Refusals

- The expectation to comply with Ontario's access laws remains in effect.
- IPC is processing Deemed Refusal appeals and will take into consideration the challenges institutions are facing to meet the 30-day time limit in the current context.

## Initiating Complaints or Appeals to the IPC

- The suspension order, under the [Emergency Management and Civil Protection Act](#) that 'froze' the time limits for initiating complaints or appeals to the IPC, expired on September 14, 2020.
- As of September 14<sup>th</sup>, the time limits for initiating complaints or appeals, as set out in the *Acts*, have resumed as normal.



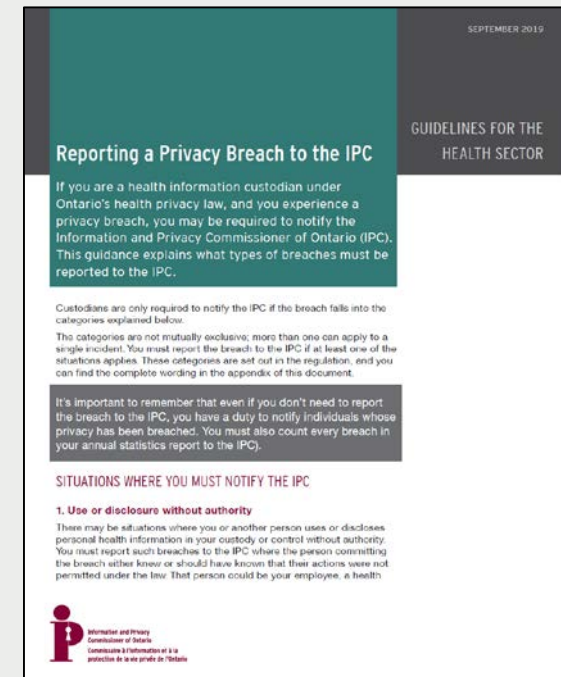
# FAQs re Impacts of COVID-19 on FOIP operations

## Requests and appeals relating to third parties

- Before disclosing any third party records, institutions should verify with the IPC to determine whether a third party appeal has been filed.

## Breach Reporting

- Institutions and organizations should continue to report privacy breaches to the IPC using the [online breach report form](#).





# Importance of Public Health Sharing

- Ontario's privacy laws are not a barrier to sharing information that is critical to public well-being and can help control virus outbreaks.
- IPC encourages public health units and other public institutions to provide as much non-identifying information as necessary to help control spread of the virus and protect public safety
- Non-identifying information could include:
  - numbers of infected individuals and/or deaths
  - demographic data such as age range and gender
  - geographic locations
  - names or types of institutions, such as, schools, long term care facilities, or workplaces, where large numbers of people might have gathered

# Police Access to COVID-19 Risk Look Up Tool

< Home **CTV NEWS**

TORONTO | NEWS

## Civil rights group finds Ontario police used COVID-19 database illegally

John Chidley-Hill  
The Canadian Press Staff  
Contact

Published Wednesday, September 30, 2020 12:32PM EDT  
Last Updated Thursday, October 1, 2020 7:41AM EDT

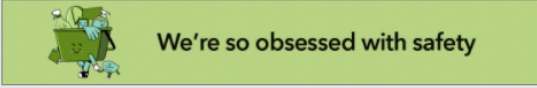


File Photo. (AP / Damian Dovarganes)

**CBC** | MENU

COVID-19 Local updates Live broadcast COVID-19 tracker Subscribe to newsletter

NEWS Top Stories Local The National Opinion World Canada

 We're so obsessed with safety

Toronto

## Ontario police used COVID-19 database illegally, civil rights groups find



Use of the portal violated individual privacy rights for months, groups say

The Canadian Press - Posted: Sep 30, 2020 6:42 PM ET | Last Updated: September 30



The Canadian Civil Liberties Association and the Canadian Constitution Foundation say in separate reports that many services used the database to look at COVID-19 test results for wide geographic areas and sometimes pulled up personal information unrelated to active calls. (maradon 333 / Shutterstock)

**TORONTO SUN**

orts Opinion Entertainment Life Sunshine Girls Driving Healthing TheGrowthOp ePage

Ontario

## Ontario police used COVID-19 database illegally: Civil rights group

 Canadian Press

Sep 30, 2020 • Last Updated 19 days ago • 2 minute read



As Torontonians adjust to life during the Covid-19 pandemic; Toronto Police continue to respond to calls, this one at 345 Bloor Street East, on Sunday March 29, 2020. PHOTO BY STAN BEHAL /Toronto Sun/



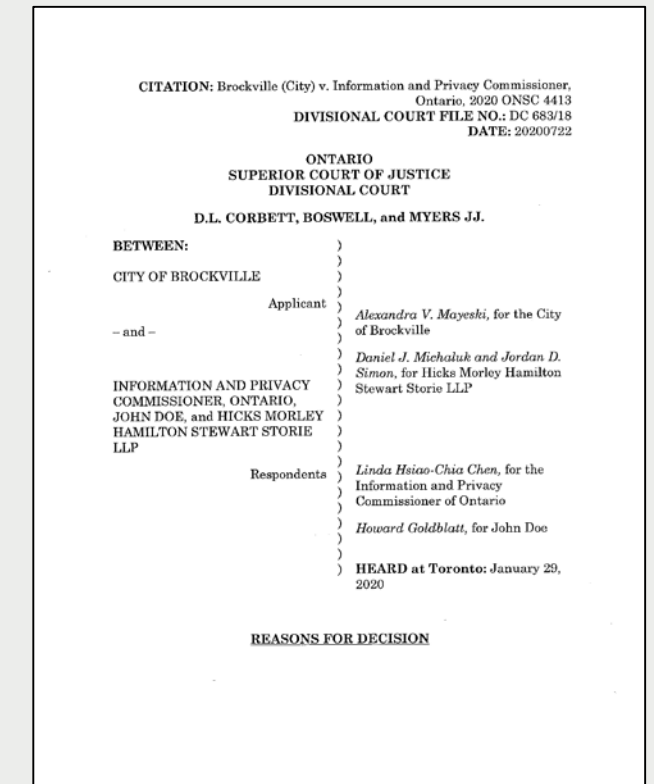
# Body-Worn Cameras

- Shifting values around police and BWCs
- Mounting public demand for police accountability and transparency
- Need to balance privacy considerations, with emphasis on context – third parties, public spaces, and surveillance
- IPC working with Toronto police services on developing policy framework and procedures for implementation of BWC program
- Hoping it will serve as useful model for other police services in Ontario



# Brockville Decision - *Brockville (City) v. IPC*

- Ontario's first FOI judicial review decision after *Canada v. Vavilov*
- Confirmed the standard of reasonableness in judicial review of IPC's decisions
- Court recognized IPC's significant experience with Ontario's access and privacy laws
- Decision could have far-reaching impact for future challenges to IPC access orders before the courts



# Premier's Mandate Letters

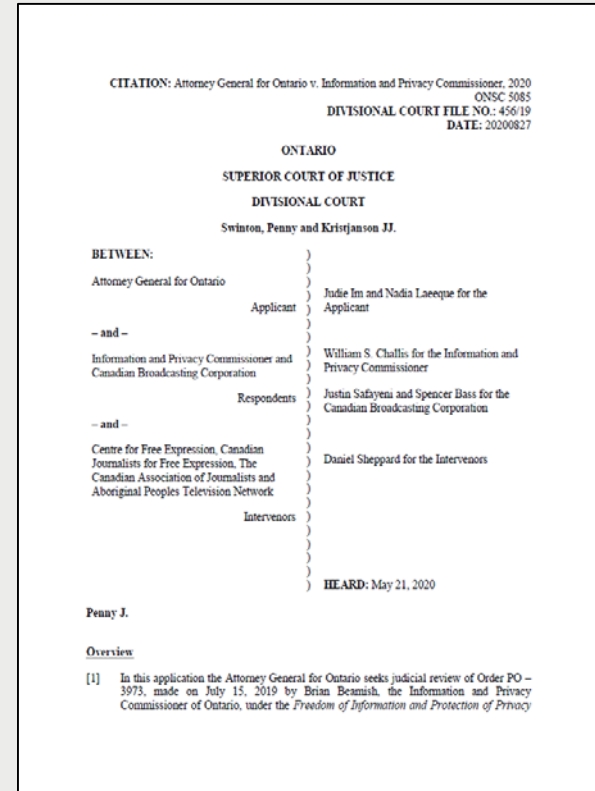
- A requester sought a copy of each of the mandate letters Premier Doug Ford sent to Cabinet Ministers for all of Ontario's ministries, and two non-portfolios.
- The Cabinet Office denied access to all the records claiming the application of the mandatory exemption in s12(1) believing that disclosure 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.



# FIPPA Amendment: Data Integration

- In 2019, FIPPA was amended to add a new data integration scheme ([Part III.1](#)).
- The provisions enable data integration units (DIUs) to indirectly collect personal information and link it with other information for the purpose of analysis related to planning and evaluation of government programs and services.
- They also define requirements related to notice of collection, data minimization, limits on use and disclosure, de-identification, security, etc.
- IPC has the power to review DIUs' practices and procedures, order them to start, stop or change a practice or procedure, as well as to destroy personal information.

# Made-in-Ontario Private Sector Privacy Law

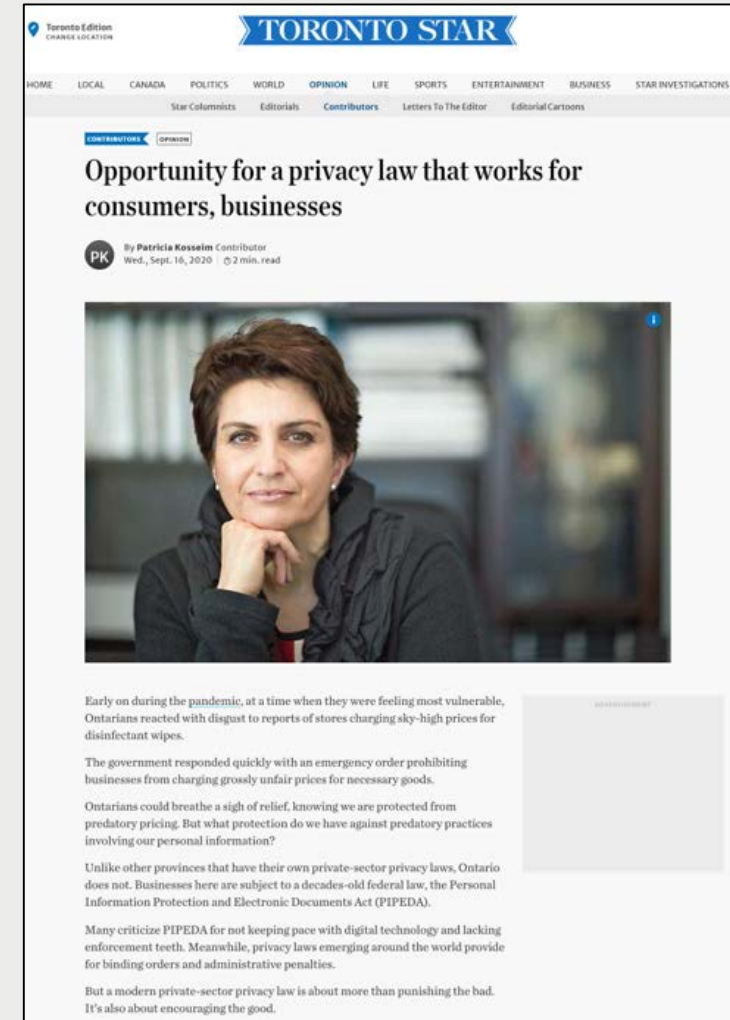
- August 13 – Ministry of Government and Consumer Services began a consultation regarding a made-in-Ontario private sector privacy law
- Key areas that the government is considering:
  1. increased transparency
  2. clear consent provisions
  3. right to deletion and de-indexing
  4. data portability
  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



# 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](#)



# Ontario's opportunity in a nutshell

- To broaden the scope of the law's application to bring other organizations into the fold, which continue to operate in a legislative vacuum due to the constitutional limits of PIPEDA;
- To level the playing field with greater certainty and more predictable rules, harmonized with that of other jurisdictions, that incentivize responsible use and respectful treatment of data, while prohibiting unfair and inappropriate data management practices;
- To design a more comprehensive and coherent regime, with a better integrated, streamlined, and agile oversight mechanism to address complex data challenges that lie at the intersection of public and private sectors;

# Ontario's Opportunity in a Nutshell

- To selectively adopt those aspects of other privacy statutes that have proven to work well over time, while replacing the less enviable elements with more effective approaches that are nevertheless harmonized and interoperable with those other laws;
- To modernize and refresh the foundational principles of a modern privacy law that provide the guardrails for responsible data processing and help support sustainable decisions and actions over time; and,
- To create a forward-looking, world-class private sector privacy law capable of rising to the emerging challenges of a digital age in a manner which, ultimately, works best for the people and organizations of Ontario and accords with local values and culture.

# 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