

Strengthening Privacy and Transparency in the Digital Age: Insights from the IPC

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

Canadian Access
and Privacy
Association

November 28, 2022

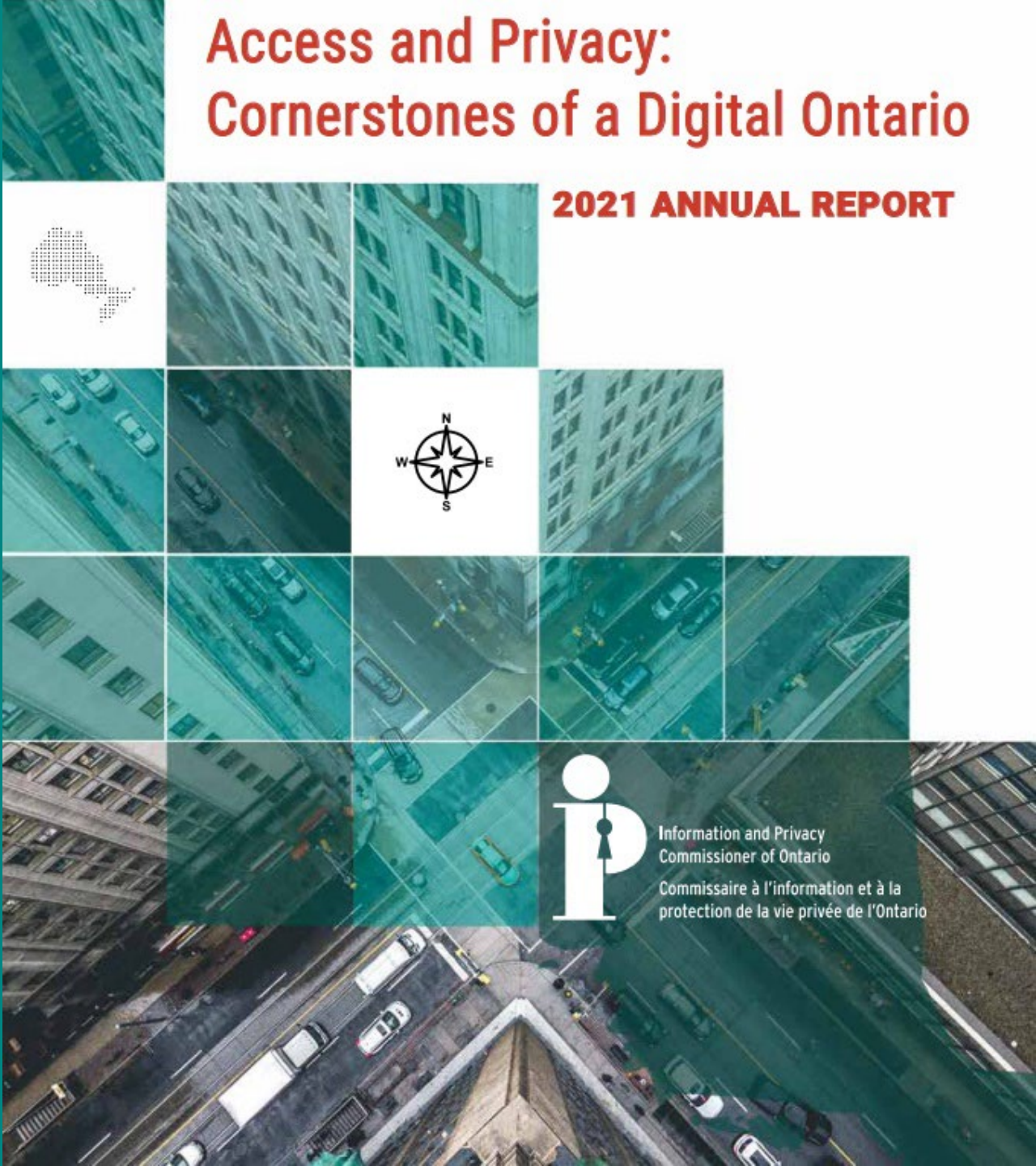
Access and Privacy: Cornerstones of a Digital Ontario

2021 ANNUAL REPORT

Information and Privacy Commissioner (IPC)

The IPC is mandated to:

- receive complaints and appeals from the public on matters of access and privacy
- offer comment on the privacy implications of proposed legislative schemes or government programs
- consult with public institutions on proposed policies or operations to help mitigate privacy risks and develop sound data management frameworks
- engage in research and conduct public education programs on access and privacy matters
- report annually to the Legislative Assembly through the Speaker



Ontario's Privacy and Access Laws

- ***Freedom of Information and Protection of Privacy Act (FIPPA)***
 - covers 300 provincial institutions, including ministries and universities
- ***Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)***
 - covers 1,200 municipal organizations, including schools and police services
- ***Personal Health Information Protection Act (PHIPA)***
 - covers individuals and organizations involved in the delivery of health care services, including hospitals and health providers
- ***Child, Youth and Family Services Act (Part X) (CYFSA)***
 - covers children's aid societies, child and family service providers
- ***Anti-Racism Act (ARA)***
 - oversight of the privacy protective rules governing the collection and use of race-based data to address systemic issues of racism

IPC Vision of a Modern and Effective Regulator

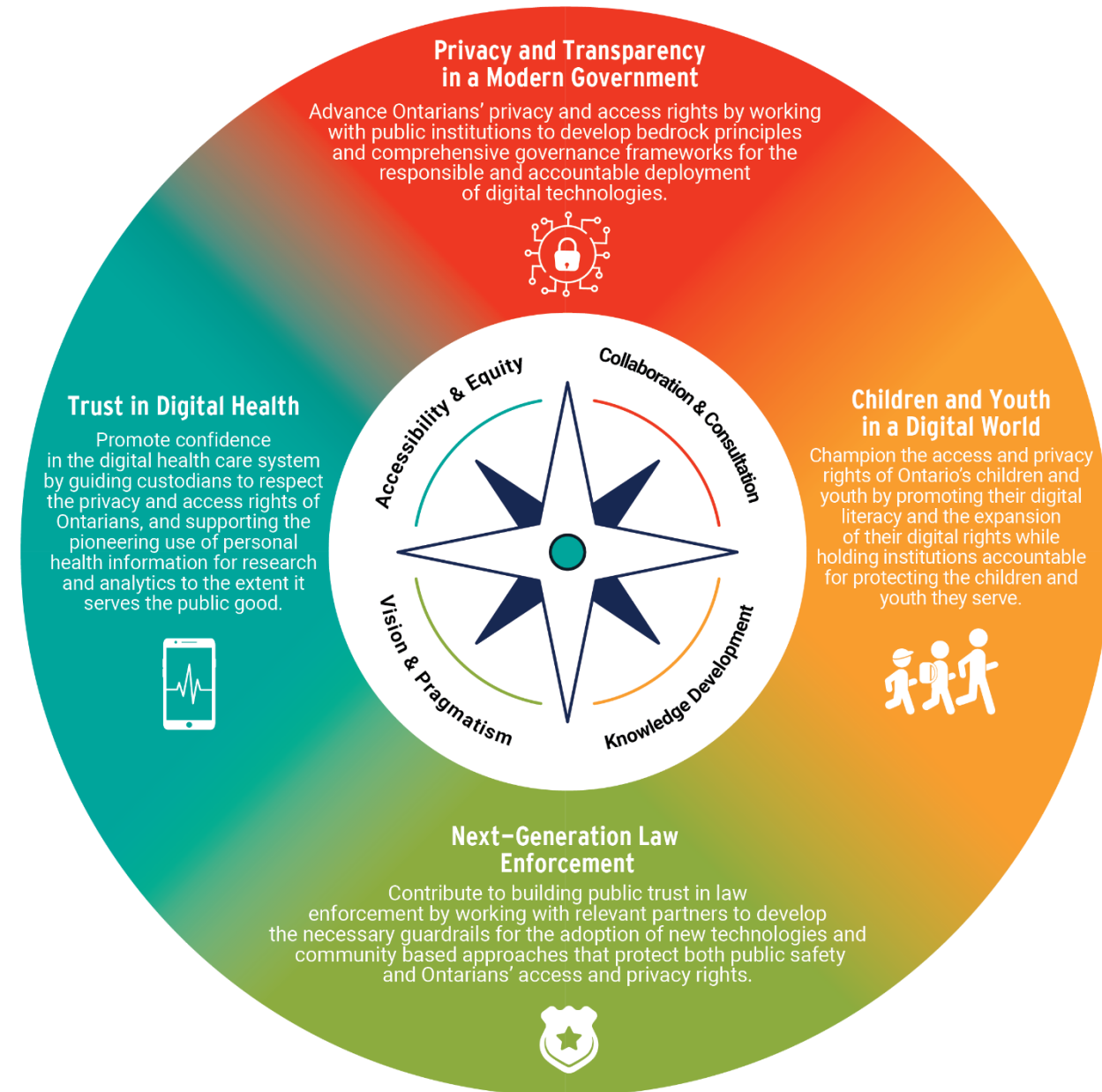
Enhance Ontarians' trust that their access and
privacy rights will be respected by ...



IPC's Strategic Priorities 2021-25

Focus on promoting and protecting Ontarians' access and privacy rights in these key areas:

1. Privacy and Transparency in Modern Government
2. Children and Youth in a Digital World
3. Next-Generation Law Enforcement
4. Trust in Digital Health





Privacy and Transparency in a Modern Government

- Digital identity
- Framework for Trustworthy AI in public sector
- New Data Authority



Children and Youth in a Digital World

- Education materials aimed at kids
- Protecting students' digital rights in schools
- Implementing Part X of the CYFSA



Next Generation Law Enforcement

- Body-worn cameras
- Facial recognition technologies
- New community-based models of policing



Trust in Digital Health

- Virtual healthcare
- Three-year reviews of prescribed entities, persons and organizations under PHIPA
- PHIPA amendments



IPC Strategic Advisory Council

- A permanent advisory council of experts from public/private sectors, academia, law, advocacy groups, health, education and law enforcement
- Members also participate on one of four priority tables, each dedicated to advancing a specific strategic priority

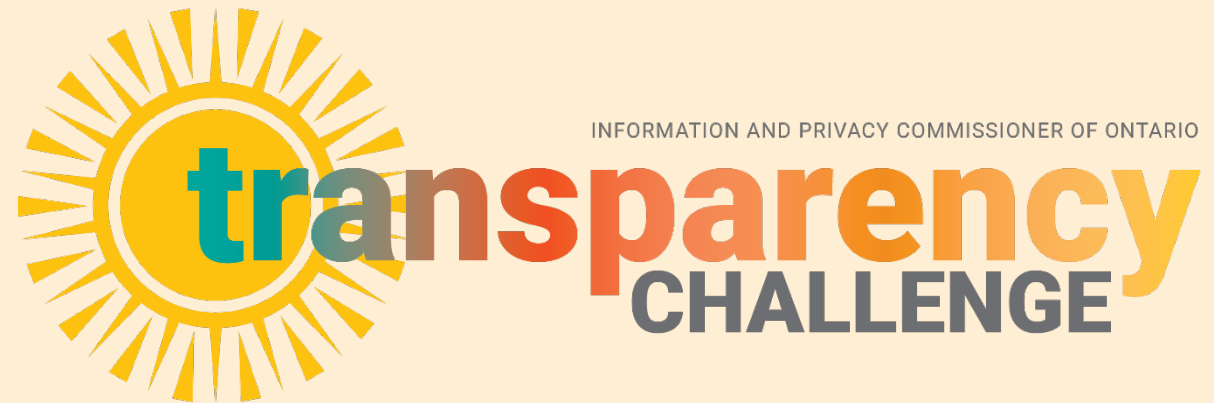
IPC Youth Advisory Council

- Members may be asked to share their opinions on:
 - Access and privacy rights of Ontario's children and youth
 - Holding institutions accountable for protecting children and youth
 - IPC program ideas and resources to enhance privacy education and digital literacy among children and youth
- Serve for a two-year term
- Email youthcouncil@ipc.on.ca for info



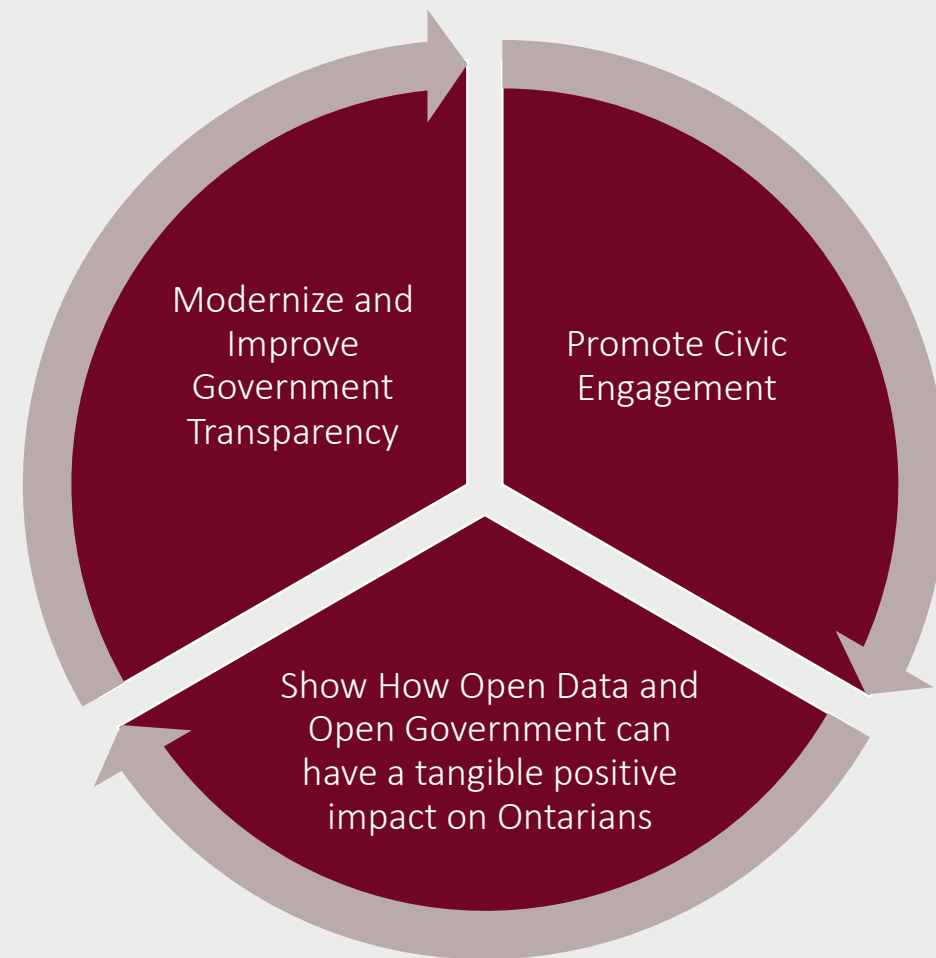
Transparency Challenge

- Launched on September 28, International Right to Know Day
- *Privacy and Transparency in a Modern Government* is one of our four strategic priorities.
- Transparency helps people understand government decision-making and the policies and issues that matter to them.
- Visit our website for more details.



Transparency Challenge

- Open to public sector institutions in Ontario at the provincial and municipal levels that are subject to FIPPA and MFIPPA
- Examples will be featured in the IPC's Transparency Showcase
- Entry Deadline: January 13, 2023



Next-Gen Law Enforcement Foresight Series

- Technological and social context of law enforcement is changing
- Need to build a shared understanding of the future for privacy and transparency
- Foresight is not about predicting the future, but exploring a range of plausible futures





National / International Resolutions

National and International Resolutions

- **Canada's FPT Commissioners (Sept '22)**
 - Axe the Fax/Secure communications in digital health care
 - Digital Identity Ecosystems
- **Global Privacy Assembly (Oct '22)**
 - Facial Recognition
 - International Cooperation on Cybersecurity



Retiring Fax Machines from Health Care Delivery

- September 2022 joint resolution by federal, provincial, and territorial regulators
- Outlines measures for adoption by governments, health institutions, and health care providers. They include:
 - A plan to phase out fax machines and unencrypted email in the delivery of patient care across Canada as quickly as possible
 - Adoption of secure digital technologies and data governance frameworks to protect personal health information against unauthorized access or inadvertent disclosure



Digital Identity Ecosystems in Canada

- October 2022 joint resolution by federal, provincial, and territorial regulators
- Privacy and transparency must be at the core of any digital ID system
- Ensure that privacy and transparency rights are fully respected throughout the design, operation, and evolution of a digital identity ecosystem in Canada



Recommendations for Digital Identity Systems

- Should be optional and accessible
- Shouldn't force people to identify themselves when it isn't necessary to access a product or service
- Only the minimum amount of personal information necessary to confirm identity should be collected, used, or shared
- People's activities shouldn't be tracked
- Must be secured from identity theft, fraud or other harms
- Governments, organizations must be held accountable for their use and subject to independent oversight



GPA Resolution on Facial Recognition Technology

- The IPC co-led the development of a resolution on principles and expectations for the appropriate use of personal information in facial recognition technology.
- The international membership adopted the resolution at this year's assembly in October 2022.
- This resolution builds on a previous resolution on facial recognition technology co-sponsored by the IPC, which GPA members adopted in October 2020.



GPA Resolution on Cybersecurity

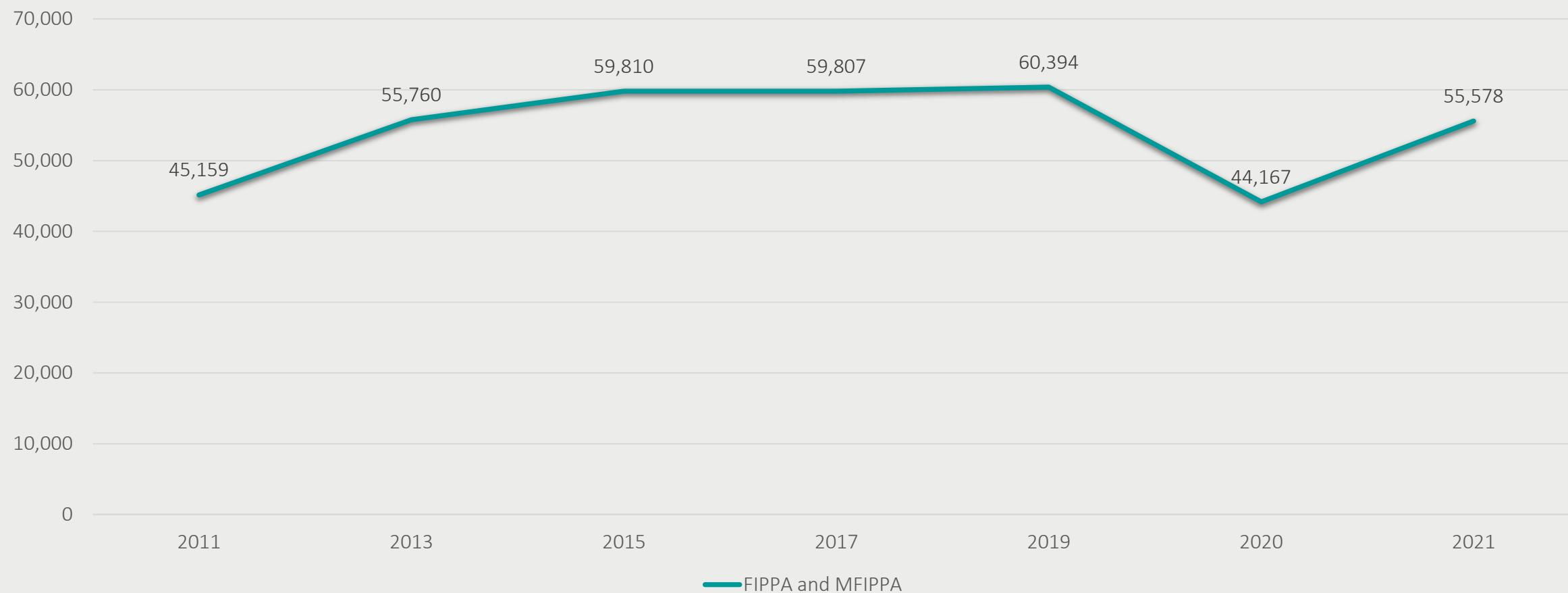
- GPA resolution on International Cooperation Capacity Building for Improving Cybersecurity Regulation and Understanding Cyber Incident Harms was adopted in October 2022.
- This resolution arose from the increasing digitalization of the global economy and along with it, the threat to individuals' personal data held by public and private organizations.
- Confidentiality, integrity and availability are three key elements of information security that are at risk.





Tribunal Update

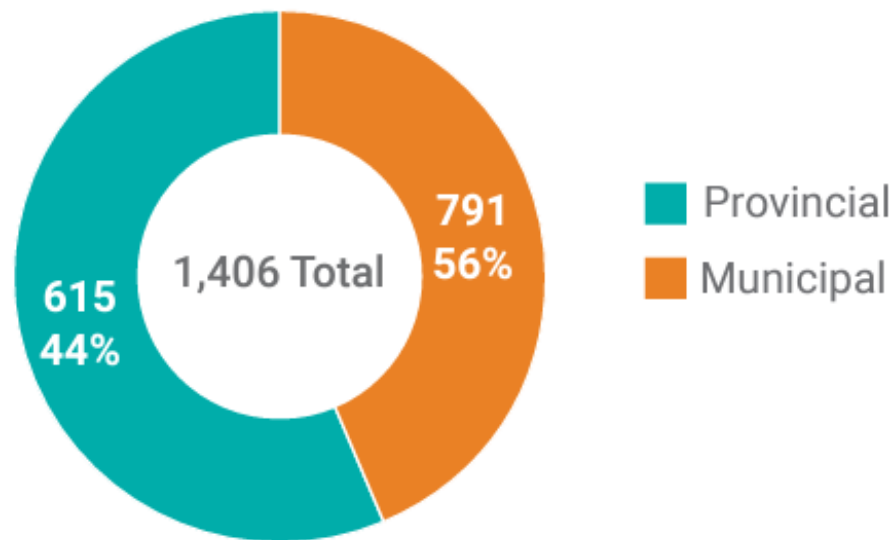
Access Requests filed under FIPPA and MFIPPA



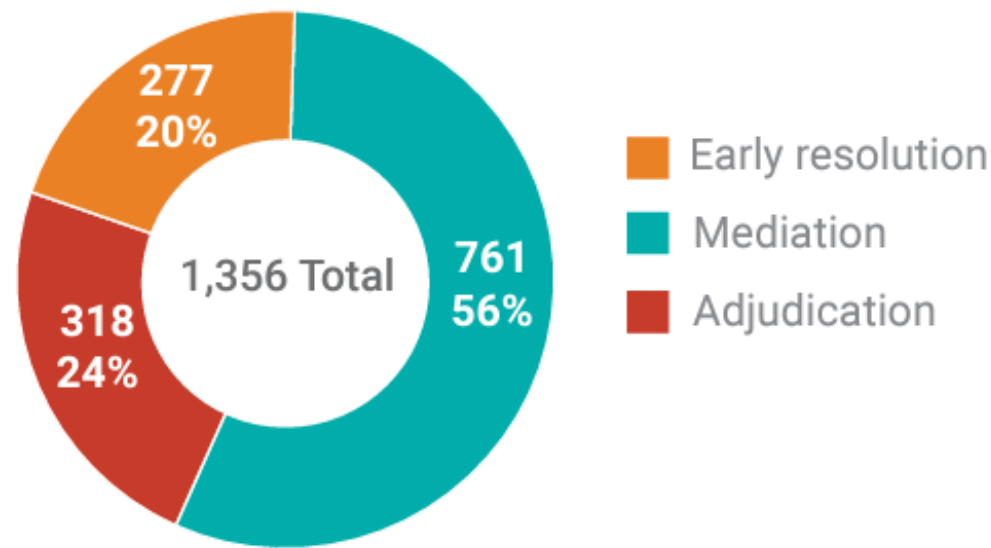
Number and Disposition of Appeals filed to the IPC, 2021

FIPPA/MFIPPA Files

Access Appeals Opened



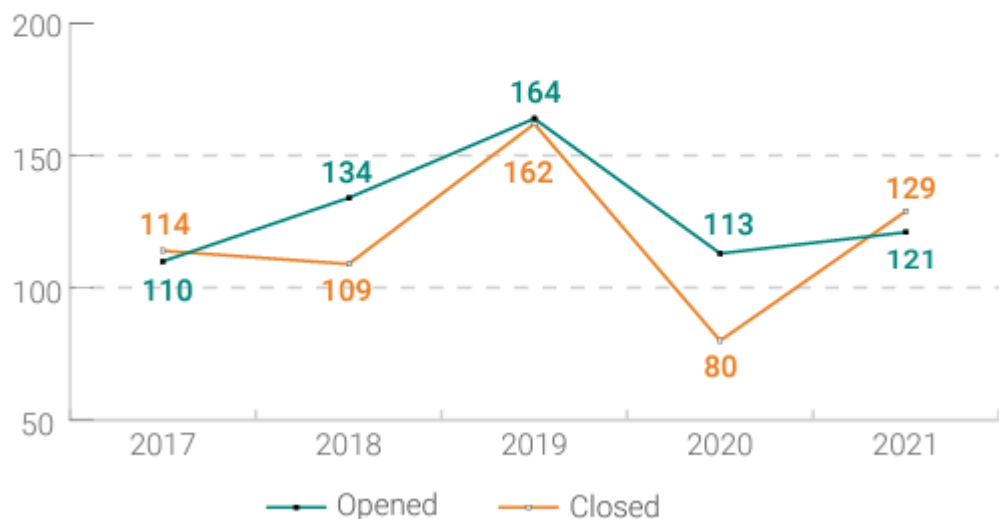
Access Appeals Resolved by Stage



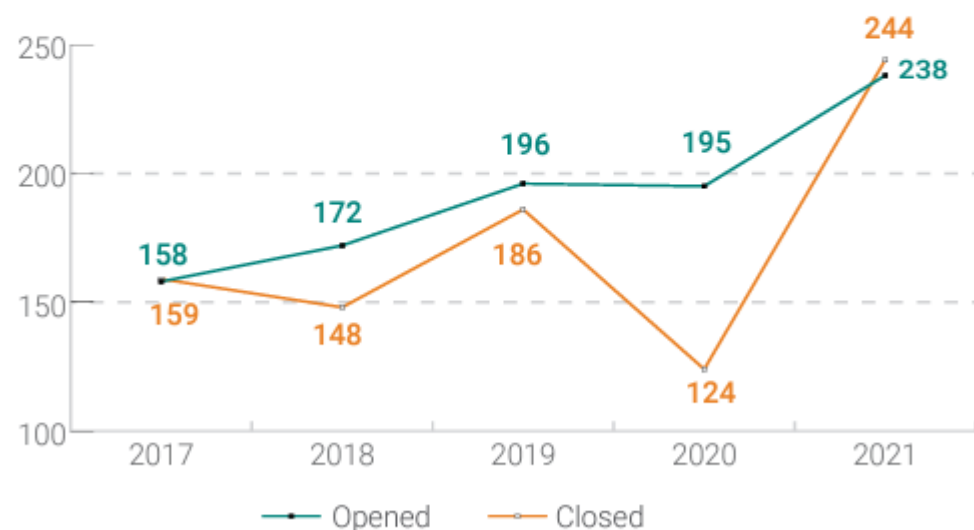
Privacy Complaint Files, 2017-2021

FIPPA/MFIPPA Files cont'd

Provincial Privacy Complaints & Self-Reported Breaches Opened/Closed 2017 – 2021

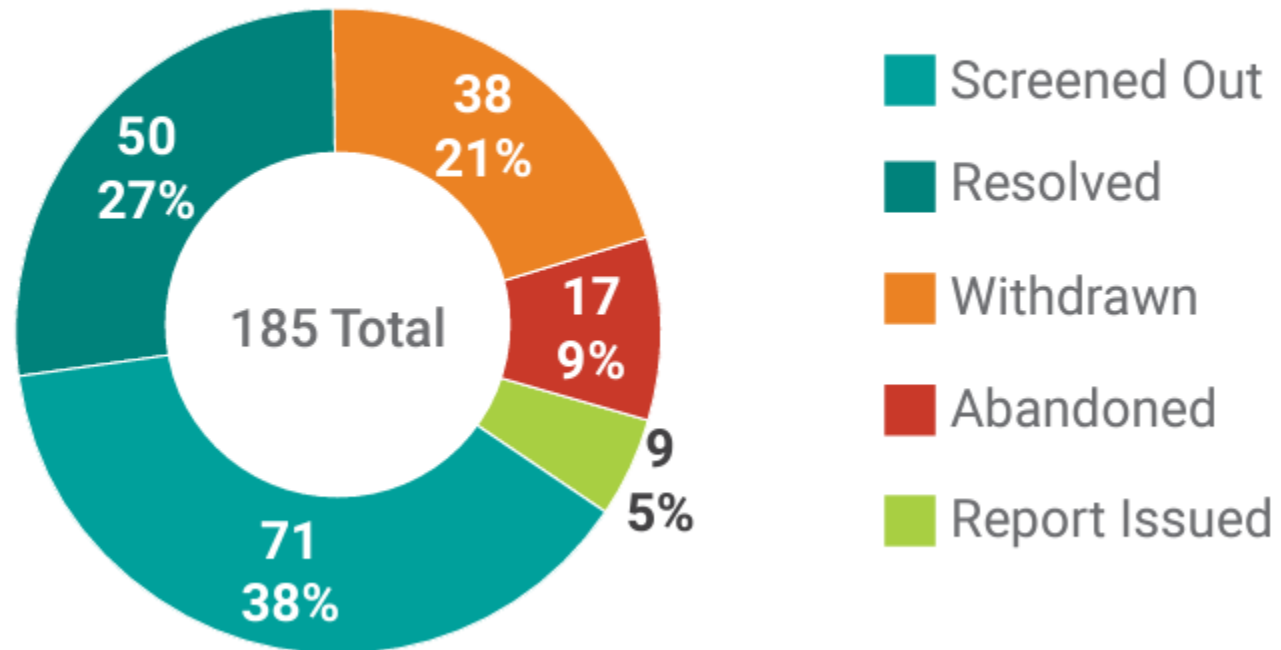


Municipal Privacy Complaints & Self-Reported Breaches Opened/Closed 2017 – 2021



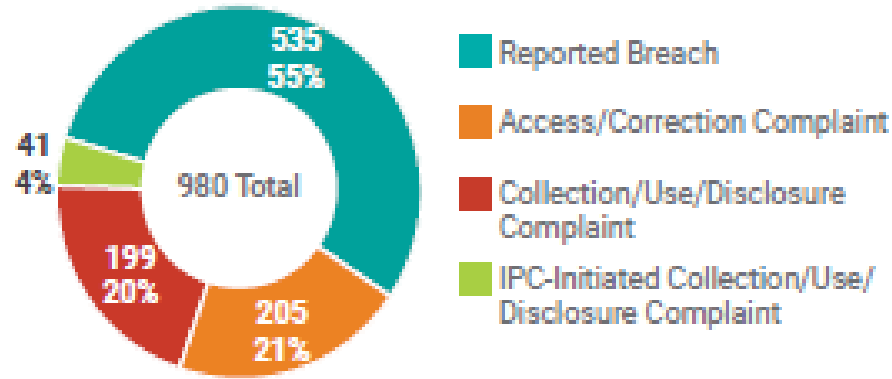
M/FIPPA Privacy Complaint Files by Resolution Type, 2021

Privacy Complaints* Closed by Type of Resolution

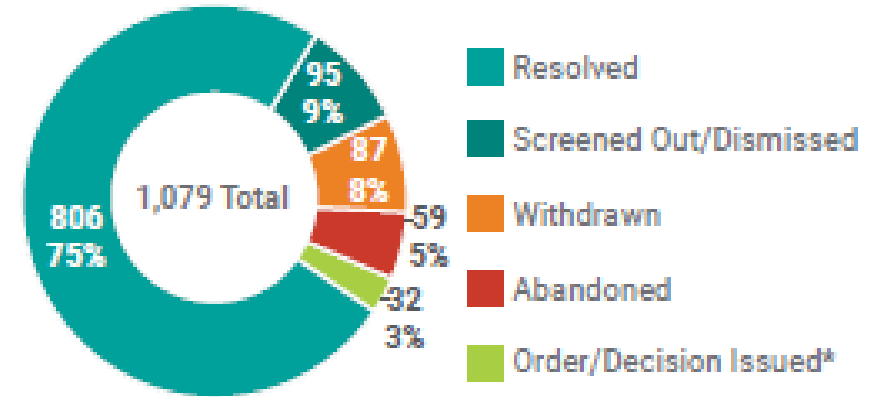


PHIPA Files, 2021

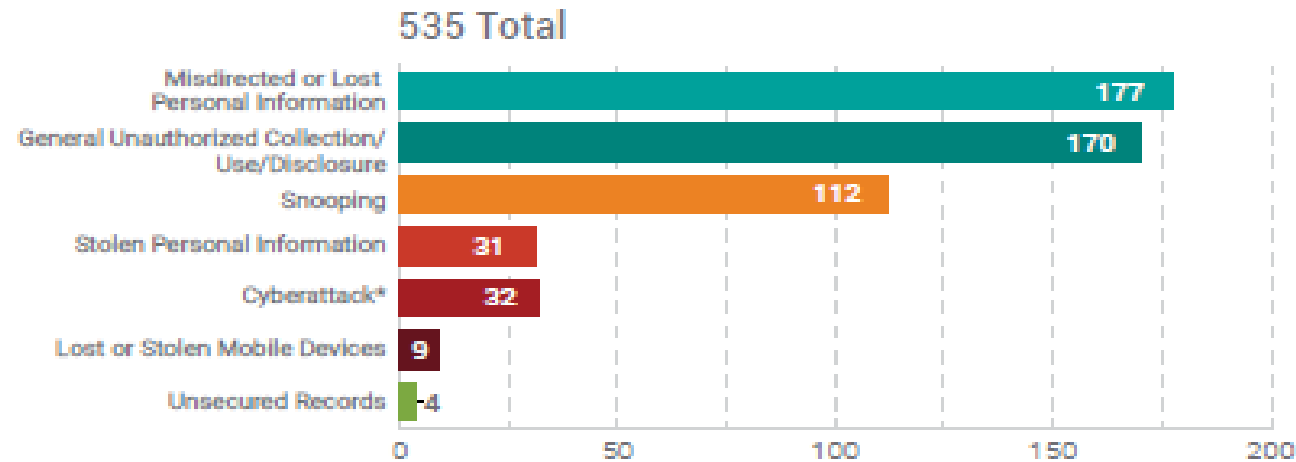
Types of Health Files Opened



Outcome of Health Files Closed



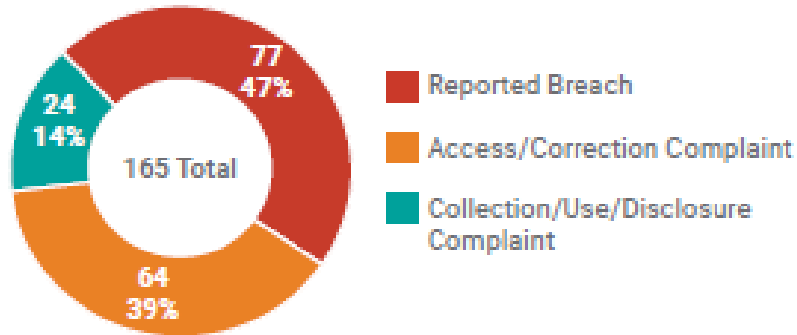
Self-Reported Health Privacy Breaches by Cause



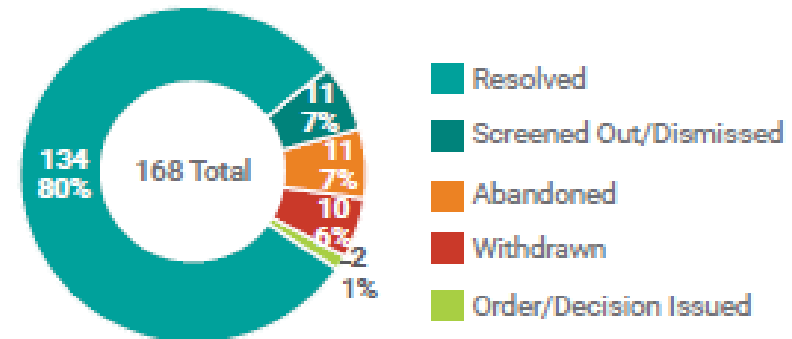
* 8 out of 32 cyberattacks involved ransomware

CYFSA Files, 2021

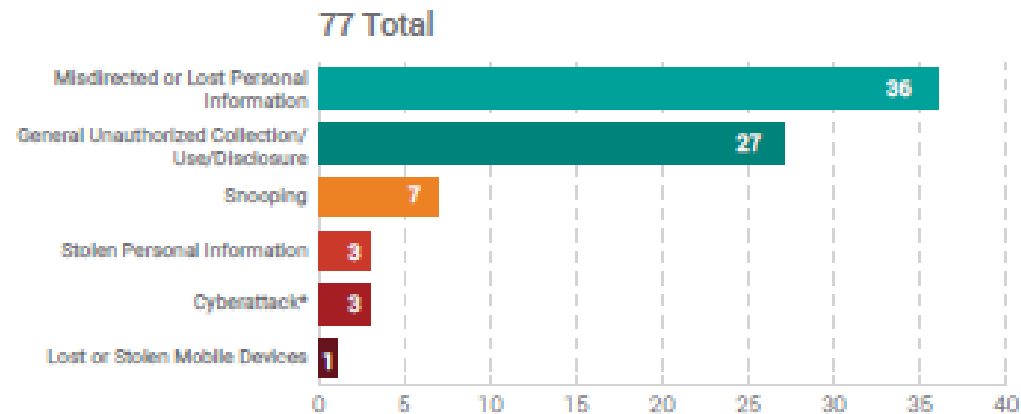
CYFSA Files Opened by Issue



Outcome of CYFSA Files Closed



Self-Reported CYFSA Privacy Breaches by Cause



* 1 out of 3 cyberattacks involved ransomware




Legislative Updates

CTV NEWS
TORONTO

TORONTO | News

Many Ontario employers now need 'electronic monitoring' policies. Here's what that means



CTV National News: Who's monitoring their workers?

Abby O'Brien
CTV News Toronto Multi-Platform
Follow | Contact

Updated Oct 11, 2022 8:49 a.m. EDT
Published Oct 11, 2022 8:19 a.m. EDT

Share

Many Ontario companies will soon have to disclose whether they're electronically monitoring their workers.

In April, Ontario became the first province to pass a **transparency law**, as part of the province's new privacy law requiring companies with 25 or more employees to have a written policy clearly outlining what data is collected from computers, cellphones, GPS systems and other devices are being tracked, and how that information is used.

POLITICO

CORONAVIRUS

Coronavirus opens door to company surveillance of workers

Privacy advocates warn of a slippery slope toward "normalizing" new levels of employer surveillance.

TORONTO STAR

CONTRIBUTORS **OPINION**

'The stuff of dystopian sci-fi': Bill 88 needs to go further to protect the privacy rights of workers

If passed, the bill would require Ontario employers to tell their workers if and how they are being monitored electronically.

By **Patricia Kosseim** Contributor
Fri., April 1, 2022 | 2 min. read

For many of us, the pandemic has changed how we work, blurring the line that used to exist between home and office. It's a radical shift that won't be rolled back anytime soon. According to a recent Ipsos poll, only half of Canadians currently working from home expect to return to the office regularly in 2022.

As employees continue to log in to work from off-site locations, employers are seeking new ways of supervising and measuring the performance of their employees remotely. But using tools like productivity monitoring software can be incredibly invasive to privacy.

In Bill 88, the Ontario government has taken a laudable first step by introducing greater transparency in this area. If passed, the bill would require employers to tell their workers if, how and in what circumstances they are being monitored electronically.

While telling workers what you're doing is good, it doesn't necessarily make it right.

From a privacy perspective, the proposed legislation doesn't go far enough. Workplace surveillance methods should be used only for fair and appropriate purposes, and only to the extent they are reasonably necessary to manage the employer-employee relationship. Employee monitoring software, or "bossware" as it is sometimes called, has serious and far-reaching capabilities. It can monitor everything from our keystrokes and mouse clicks, to our emails and video calls. It can even analyze our facial expressions to interpret — and sometimes nudge — our emotions and behaviours.

There is also the ability to track employee movements and activities remotely through tools like GPS, telematics, wearables, digital health apps and biometric timekeeping software.

It's the stuff of dystopian sci-fi movies. Things we never thought possible are being adopted in today's workplace, raising serious concerns about the lack of privacy protection for Ontario employees.

Electronic workplace monitoring should ultimately be governed by a more comprehensive Ontario private sector privacy law, similar to what was boldly proposed last year in the government's white paper on modernizing privacy in our province.

Employees should have a place to complain when their employer doesn't comply with workplace monitoring policies, and have recourse if they're unduly harmed by them.

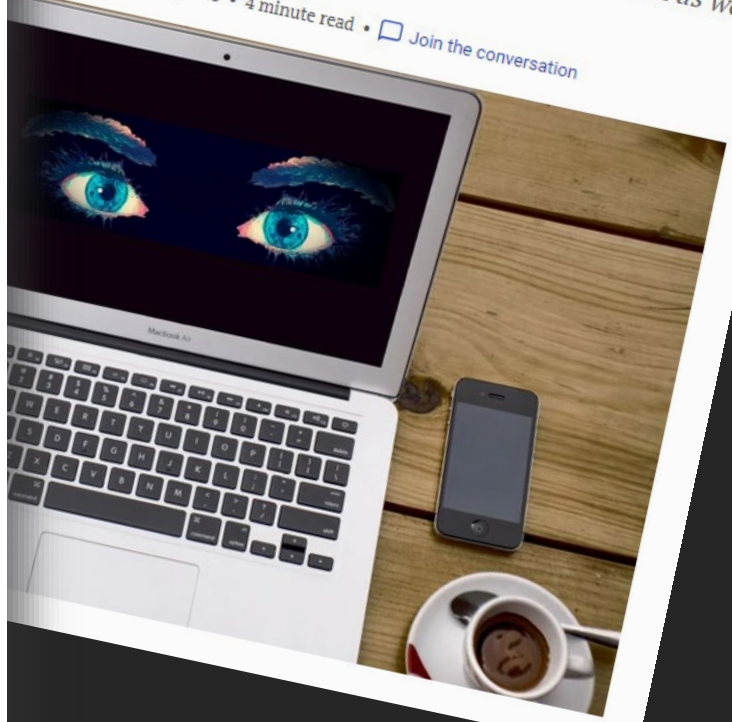
NATIONAL POST

Full Comment

Vass Bednar: Your boss is watching you while you work

Electronic surveillance in the workplace is nothing new, but it's becoming more sophisticated and alarmingly common as we work remotely

Vass Bednar, National Post
August 18, 2020 • August 18, 2020 • 4 minute read • Join the conversation



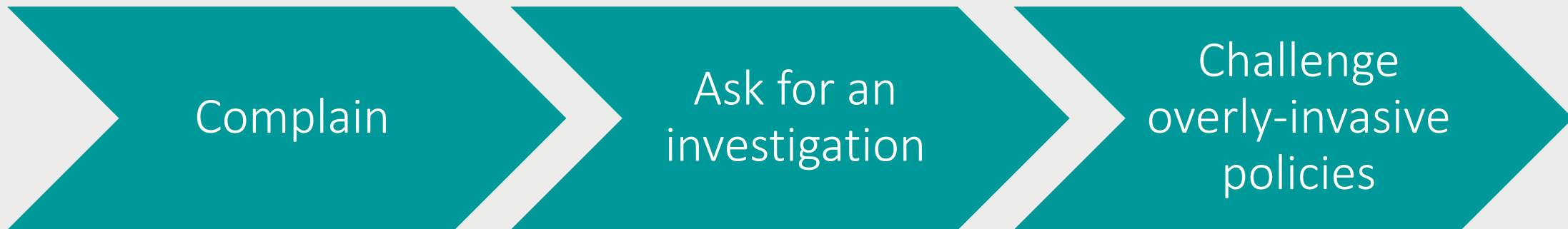
Bill 88, Working for Workers Act, 2022

- Schedule 2 amends the *Employment Standards Act* (ESA) which requires employers with 25 or more employees to have a written policy explaining whether, how, and in what circumstances they monitor workers electronically as well as the purposes for which they intend to use the information collected.
- It also permits the Lieutenant Governor in Council to prescribe by regulation, among other things, additional requirements for electronic monitoring policies, terms or conditions of employment related to electronic monitoring, and prohibitions related to electronic monitoring.
- Under the amendments, employers must have written policy in place by October 11, 2022 and provide a copy of the policy to employees by November 10, 2022.

Legislative Gaps in Bill 88

Transparency alone is not sufficient. Accountability too must be strengthened by allowing workers to do something with those policies.

- Workers should be able to:



PHIPA Administrative Penalties

- Significant changes made to the *Personal Health Information Protection Act* (PHIPA) in 2020 to align with the move toward digital health in Ontario
- One amendment gave the IPC the power to impose administrative penalties against persons who contravene *PHIPA*
- Purpose of administrative penalties is to (a) encourage compliance with the Act or (b) prevent a person from deriving, directly or indirectly, any economic benefit as a result of contravening the Act.
- Regulations setting out how amounts shall be determined must first be adopted before IPC can begin imposing administrative penalties

Role of a Modern and Effective Regulator

- The IPC is working with partners and stakeholders on clearly defining, in measurable terms, what it means to be a modern and effective regulator
- We are considering the ways that we can continue to improve effectiveness by considering the value-add of innovative regulatory approaches
- Ongoing stakeholder engagement and consultation with regulated sectors, subject matter experts, and members of the public will be a core component of this work





Consultation, Public Education and Outreach

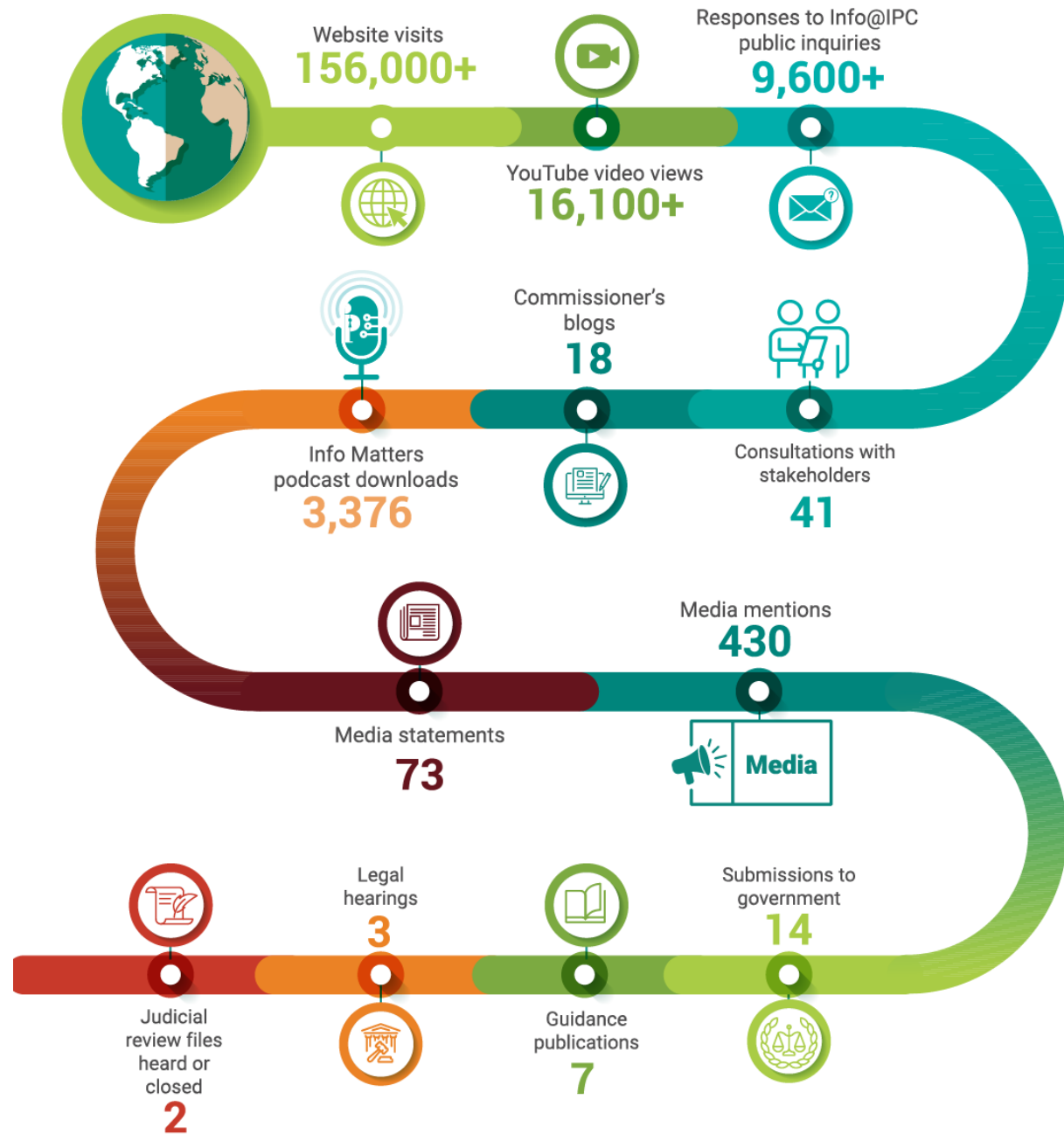
IPC Policy Consultations

To help promote a culture of openness and transparency, the IPC has issued new stakeholder guidance on our website

www.ipc.on.ca/about-us/policy-consultations/



IPC by the Numbers, 2021



IPC Publications

TECHNOLOGY FACT SHEET
FEBRUARY 2018

Disposing of Your Electronic Media

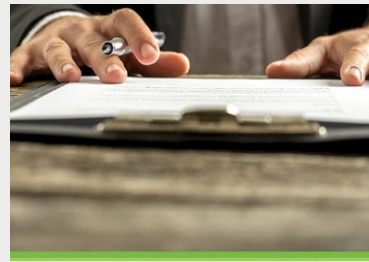
This fact sheet provides guidance on how Ontario public institutions and health information custodians can securely destroy personal information when disposing of electronic media.



Detecting and Detering Unauthorized Access to Personal Health Information



Planning for Success: Privacy Impact Assessment Guide



Open Contracting: Proactive Disclosure Of Procurement Records

TECHNOLOGY
MAY 2017

Big Data Guidelines



Guidelines for the Use of Video Surveillance

October 2015

LEGAL OBLIGATIONS
Ontario's Freedom of Information and Protection of Privacy Act (FIPPA), its municipal counterpart, MPPMA, and the Personal Health Information Protection Act (PHIPA) require institutions and health information custodians ("custodians") to take reasonable steps to safeguard personal information, including personal health information, from the moment of collection to the point of destruction.

Whether it's every day or once in a while, the question is: how do you make it follow?

TECHNOLOGY FACT SHEET

How to Protect Against Ransomware

Ransomware is a top threat facing Ontario organizations. Ransomware attacks can destroy vital records, shut critical systems and services, and put sensitive information into the hands of criminals. Organizations subject to Ontario's access and privacy laws must ensure that their cybersecurity programs include reasonable measures to protect their information. This fact sheet is meant to be a useful tool for organizations and the people they serve.

EDUCATION
JANUARY 2019

A Guide to Privacy and Access to Information in Ontario Schools

WHAT IS RANSOMWARE?
Ransomware attacks involve the digital extortion of an organization. Attackers gain control of an organization's data holdings and to take damaging action unless they receive payment. Most attacks involve at least one of the following tactics:

- **Lock out.** Attackers gain control of business-critical systems, and backups. They also use tools such as to lock an organization out of its own information and refusing to restore access until they receive payment.
- **Data theft.** Attackers gain access to large volumes of copy these records to a location they control, and then publish them unless they receive payment.

The Canadian Centre for Cybersecurity reports that ransomware attacks that affected Canadian organizations in 2020 totalled 1,000. This number is thought to be much higher because of under-reporting. A 2020 TELUS survey of 400 Canadian businesses



De-identification Guidelines for Structured Data

Model Governance Framework for Police Body-worn Camera Programs in Ontario



TECHNOLOGY FACT SHEET
JULY 2019

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.

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

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

PRIVACY FACT SHEET
JULY 2020

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.

PRIVACY

Privacy Breaches Guidelines for Public Sector Organizations

PRIVACY

Frequently Asked Questions Personal Health Information Protection Act

Reporting a Privacy Breach to the Commissioner

To strengthen the privacy protection of personal health information, the Ontario government has amended the Personal Health Information Protection Act (the Act). Under section 12(3) of the act and its related regulation, custodians must notify the Information and Privacy Commissioner of Ontario (the Commissioner) about certain privacy breaches. This law takes effect October 1, 2017.

PRIVACY

GUIDELINES FOR THE HEALTH SECTOR

PRIVACY

Part X of the Child, Youth and Family Services Act: A Guide to Access and Privacy for Service Providers



Guidance on the Use of Automated Licence Plate Recognition Systems by Police Services

Visit www.ipc.on.ca for more

Ransomware Fact Sheet

- Recently updated and reissued
- Cyberthreats are constantly changing and evolving
- Tips to avoid common traps through increased awareness and prevention

How to Protect Against Ransomware

Ransomware is a top threat facing Ontario organizations. Ransomware attacks can destroy vital records, knock out critical systems and services, and put sensitive information into the hands of criminals.

Organizations subject to Ontario's access and privacy laws must ensure that their cybersecurity programs include reasonable measures to protect their information holdings. This fact sheet is meant to be a useful overview for organizations and the people they serve.

This guide by the Office of the Information and Privacy Commissioner of Ontario (IPC) is for informational purposes only and should not be relied upon as a substitute for the legislation itself, or as legal advice. It is intended to enhance understanding of rights and obligations under Ontario's access and privacy laws. It does not bind the IPC's Tribunal that may be called upon to independently investigate and decide upon an individual complaint or appeal based on the specific facts and unique circumstances of a given case. For the most up-to-date version of this guide, visit www.ipc.on.ca.

WHAT IS RANSOMWARE?

Ransomware attacks involve the digital extortion of an organization. Attackers gain control of an organization's data holdings and often threaten to take damaging action unless they receive payment. Most ransomware attacks involve at least one of the following tactics:

- **Lock out.** Attackers gain control of business-critical systems, file repositories, and backups. They also use tools such as encryption to lock an organization out of its own information and systems, refusing to restore access until they receive payment.
- **Data theft.** Attackers gain access to large volumes of information, copy these records to a location they control, and threaten to publish them unless they receive payment.

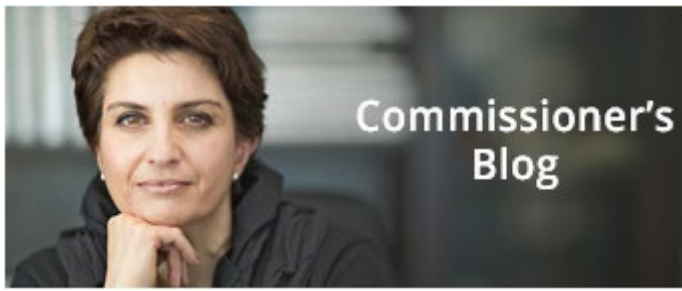
The Canadian Centre for Cybersecurity **reports** having knowledge of 235 ransomware attacks that affected Canadian organizations in 2021. The actual number is thought to be much higher because of underreporting. For example, a **2022 TELUS survey** of 463 Canadian businesses found that 83

IPC Videos and Webinars

The screenshot shows the YouTube channel page for the Information and Privacy Commissioner of Ontario. The channel name is "Information and Privacy Commissioner of Ontario" and it has a "SUBSCRIBE" button. The "VIDEOS" tab is selected, showing a grid of uploads. The uploads include:

- Privacy Tips for Kids #shorts (1:01)
- Protégez-vous contre l'hameçonnage (1:19)
- Le droit à la vie privée en matière de santé (1:28)
- Protégez votre vie privée en ligne (1:03)
- Conseils sur la vie privée pour les enfants (1:17)
- Droits d'accès à l'information (1:04)
- Health Information Privacy Rights (0:53)
- Protect Against Phishing (1:01)
- Privacy Tips For Kids (1:03)
- Access to Information Rights (1:12)
- Protect Your Privacy Online (37:46)
- Webinar: Access, correction, and breach statistics (Part X of CYFSA) (Thursday, February 10, 2022 10-11 a.m.) (34:01)
- Webinar: PHIPA Access and Correction Statistics... (Thursday, January 27, 2022 10-11 a.m.) (40:56)
- Webinar: PHIPA Breach Statistical Reporting (Thursday, January 20, 2022 10-11 a.m.) (40:41)
- Journée de la protection des données 2022 : Former une... (1:55:38)
- Privacy Day 2022 Webcast: Empowering a New... (1:56:38)
- Protecting Student Privacy Rights in Ontario (20:38)





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

Ransomware: An ounce of prevention is worth a pound of cure

Oct 13 2022

It takes years to build a reputation people can trust and seconds for a cyberattack to bring it all crashing down. Once criminals gain access to an organization's systems and the information stored within, the door is open to identity theft, economic loss, and devastating reputational damage. G...

Transparency shines bright during Right to Know Week 2022

Sep 26 2022

For Canadians, Right to Know Week is a time to reflect on our access rights and the importance of open, transparent government. This week, the IPC will spread the word about the public's right to know by sharing resources about how individuals can exercise their access rights and how public ins...

IPC welcomes Professor Teresa Scassa as its first Scholar-in-Residence!

Sep 06 2022

Guest blog by Teresa Scassa It is no secret that Ontario faces many challenges when it comes to privacy and data governance today. Some of these relate to ongoing efforts to ensure that our personal data and personal health information are properly stewarded in the public and healthcare sectors, ...

Going digital: IPC now receives FOI appeals and payments online, anytime!

Aug 10 2022

If you've read the IPC's 2021 Annual Report, you'll know that my office has set its sights on a vision to enhance Ontarians' trust that their access and privacy rights will be respected. This vision rests on three key pillars: actively advancing Ontarians' rights in key strategic areas...

Privacy and humanity on the brink

Jul 21 2022

Certain events in life are of such seismic proportion that they remind us of our fragility not only as human beings, but as an entire human species. I first got that feeling in the chaotic aftermath of 9/11 when I feared possible nuclear retaliation might put an end to us all. I felt it again whe...





Conversations about people, privacy, and access to information. Hosted by Patricia Kosseim, Information and Privacy Commissioner of Ontario.



Info Matters

Information and Privacy Commissioner of Ontario

Government

★★★★★ 5.0 • 5 Ratings

Listen to the podcast:
www.ipc.on.ca/media-centre/info-matters-podcast/

OCT 25, 2022

Seeing privacy through an equity lens in the child welfare sector >

We all have a role to play in supporting vulnerable children, youth, and families in our communities. Misunderstandings about privacy can sometimes make people hesitant to share information about potential abuse or neglect with a children's aid society. On the flip side, overreporting can lead to...

▶ **PLAY** 36 min

SEPT 30, 2022

From high school to university: a young person's perspective on digital... >

In today's connected world, children and youth are growing up online, spending more time in front of screens than any generation before them. This episode explores how young people are using digital technologies, what they think about privacy, and how parents, teachers, and regulators can help the...

▶ **PLAY** 19 min

AUG 2, 2022

Giving foster kids a fair shot in life >

Child welfare records can follow kids even after they've aged out of the system. That's the reality former foster kids face as they begin their adult lives, shadowed by deeply personal histories recorded in files that are accessible to others. This can affect their job prospects, their chance of...

▶ **PLAY** 36 min

MAY 31, 2022

In conversation with Jim Balsillie: Data, technology, and public policy >

Data is the engine of the modern economy, a key driver of innovation and growth. While the power of data is undeniable, questions emerge about the impact of digital transformation on our human rights, our collective well-being, and the state of our democracy. Commissioner Kosseim speaks with Jim...

▶ **PLAY** 29 min

IPC on Instagram



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