Freedom of Information and Privacy at the IPC

Patricia Kosseim, Information and Privacy Commissioner of Ontario
Warren Mar, Assistant Commissioner, Tribunal and Dispute Resolution

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

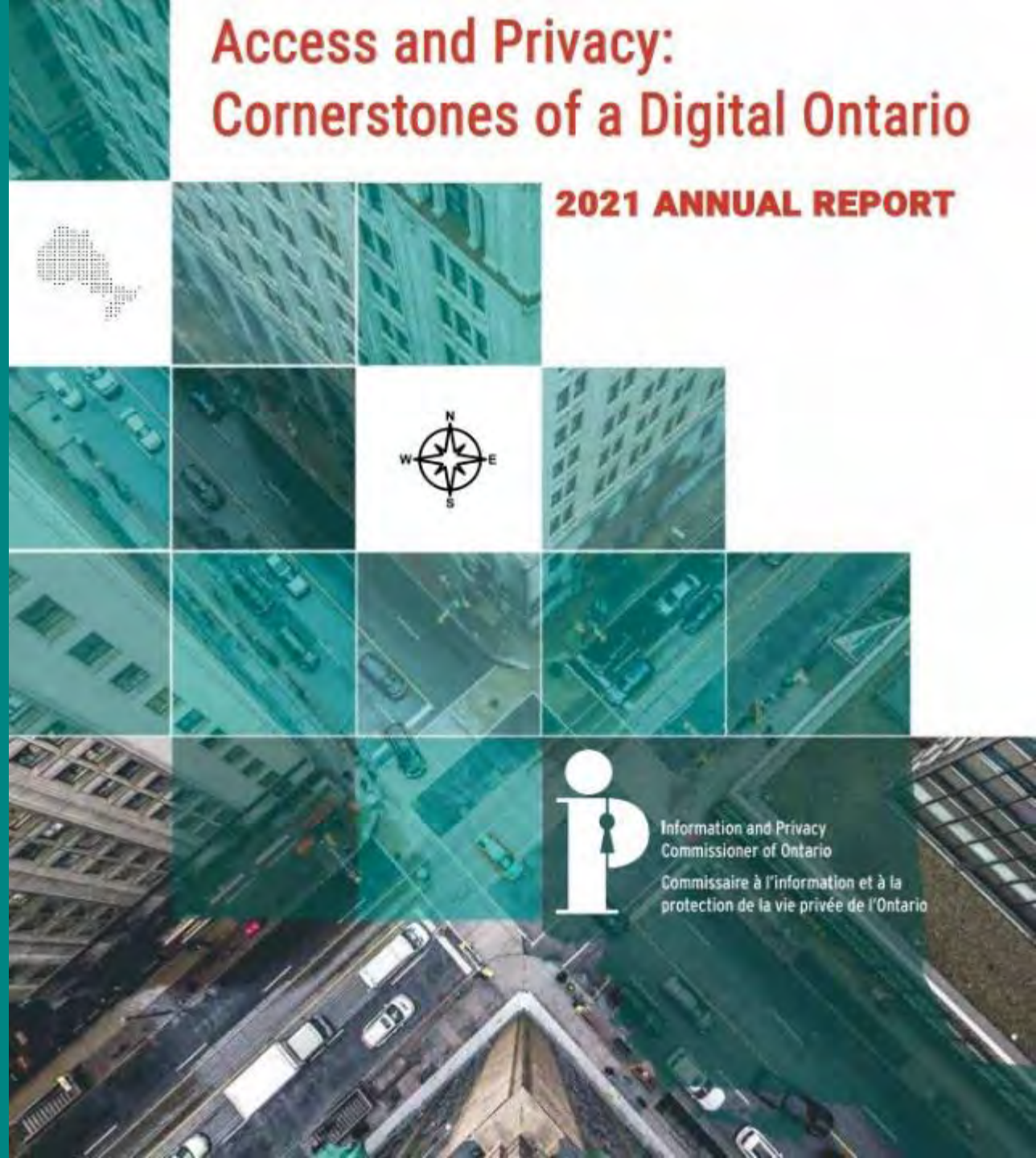
ONTARIO LEGISLATURE INTERNSHIP PROGRAMME

November 4, 2022

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

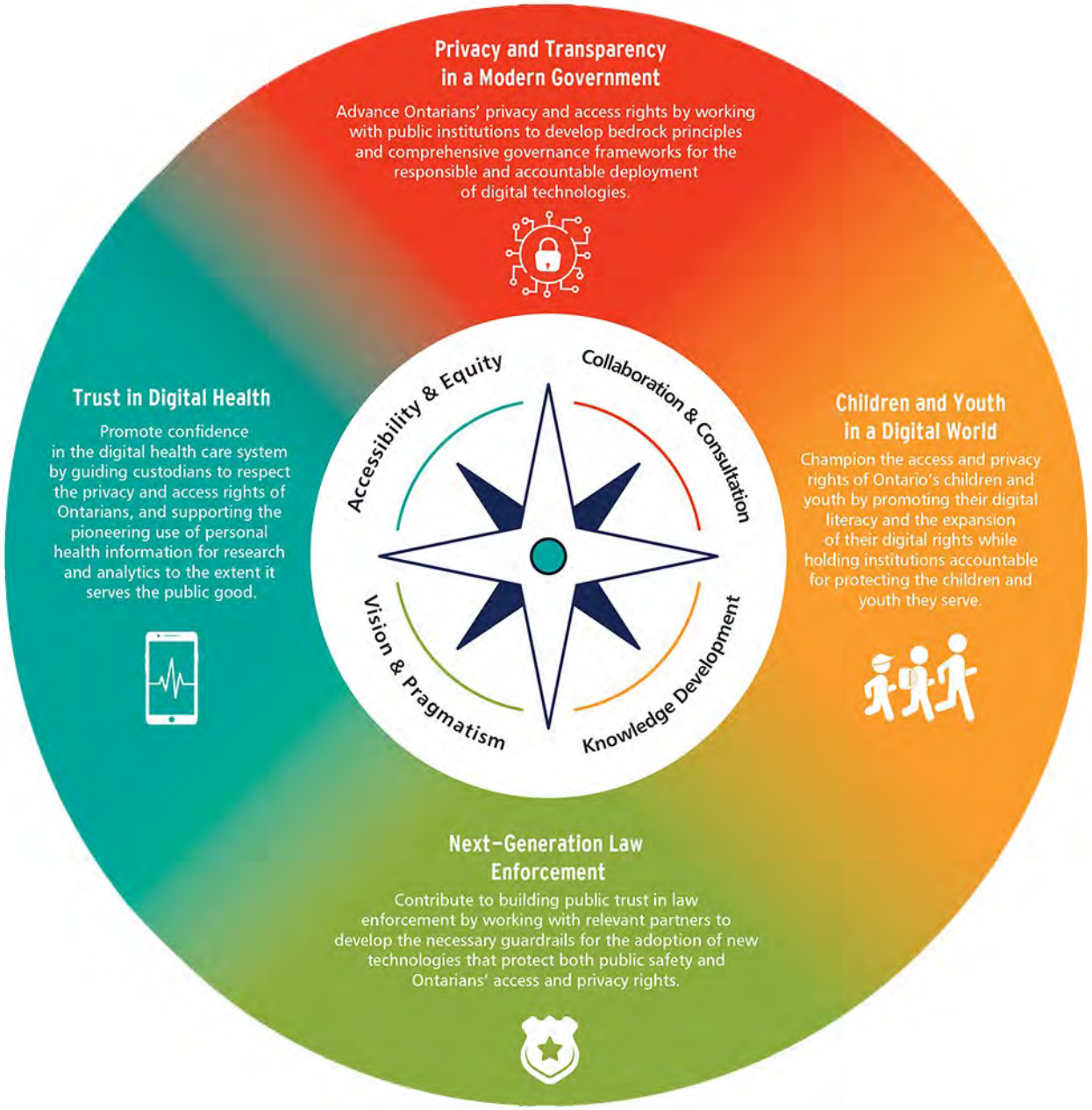
- ***Freedom of Information and Protection of Privacy Act* (*FIPPA*)**
  - covers 300 provincial institutions, including ministries and universities
- ***Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)**
  - covers 1,200 municipal organizations, including schools and police 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/youth 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

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**



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

- A group of ten young people between the ages of 15 and 24
- 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
- Selected council members can serve for a two-year term
- Application deadline: November 25, 2022
- Email youthcouncil@ipc.on.ca for info

Tribunal and Dispute Resolution

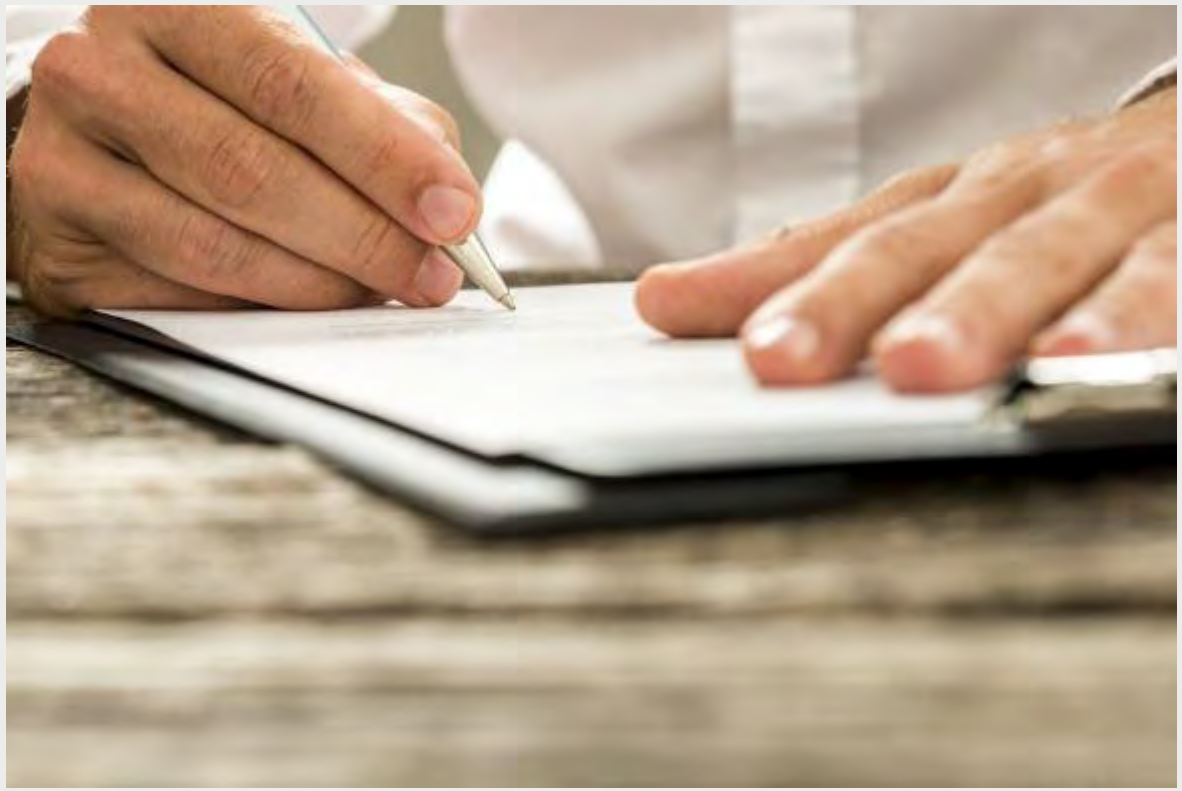
Principles of Access

Ontario's access legislation sets out basic access principles:

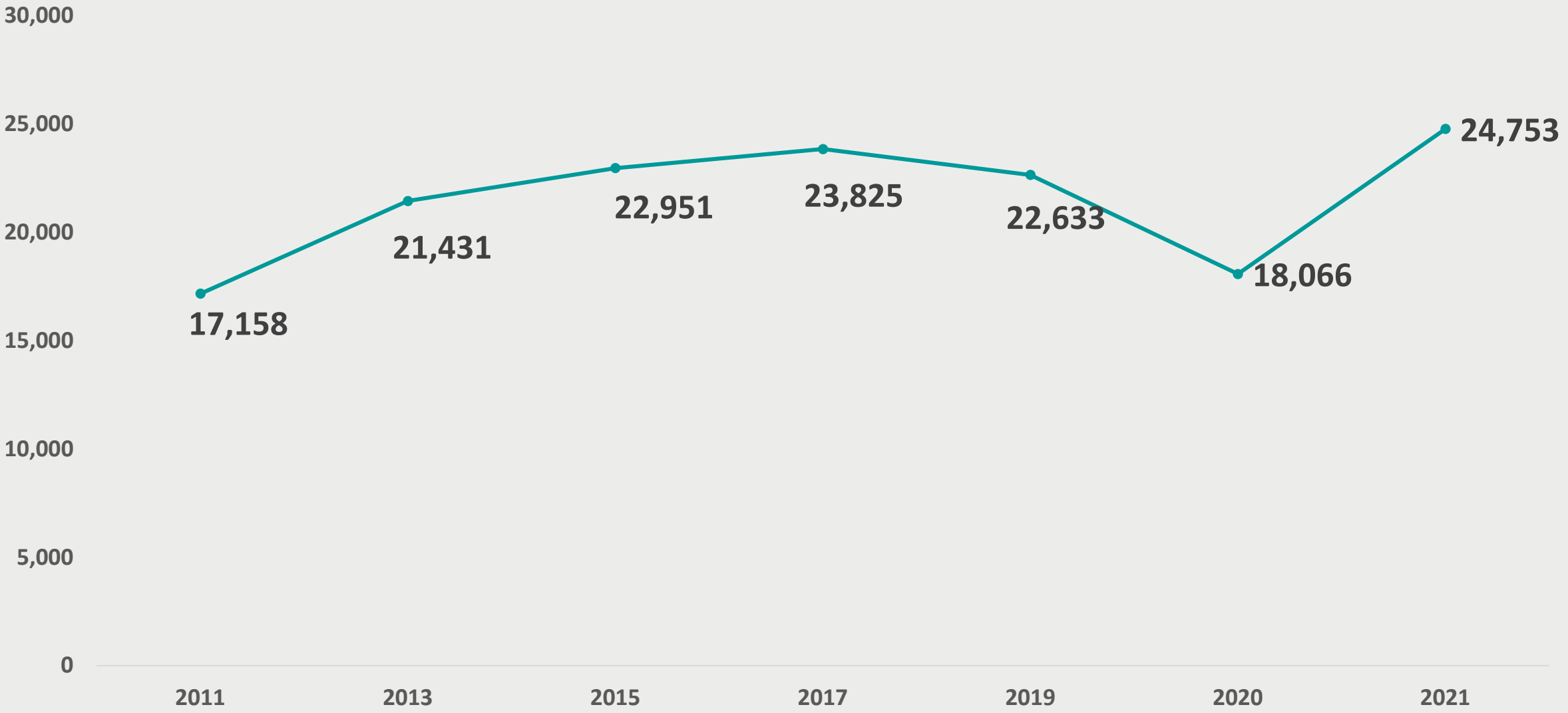
- Information under the control or custody of institutions should be made available to the public
- Exemptions from the right of access (e.g. solicitor-client privilege, Cabinet confidences, and economic interests) should be limited and specific
- When challenged, institutions' decisions in response to access to information requests should be reviewed independently

Access to Information Requests under FIPPA/MFIPPA

- Three types of requests:
  - Access to general information
  - Access to one's own personal information
  - Request to correct personal information about oneself
- Institutions must respond to a request within 30 days, subject to possible extension in specific circumstances



Number of access requests filed under FIPPA



Right of Appeal to the IPC

- A requester may appeal a decision of the institution, including:
  - a denial to provide access
  - a denial to correct personal information
  - the amount of fee charged or a refusal to waive fee
  - taking an extension of time to respond beyond the 30 day time limit
  - failure to provide any response within 30 days (“deemed refusal”)

- A third-party may also appeal an institution’s decision to disclose information that affects its interests

Stages of the IPC Appeal Process For FIPPA/MFIPPA

Early Resolution and Mediation Process

Early Resolution

- FOI appeals can potentially be resolved at the Early Resolution Stage
- If early resolution is not possible, IPC analysts have delegated authority from the Commissioner to dismiss files in appropriate circumstances or decide if the file should continue to further stages of the appeal process

Mediation

- Mediation is the process by which the IPC investigates the circumstances of an appeal and attempts to effect either a full settlement of all issues between the parties or to simplify a file by helping to clarify or settle some of the issues

Mediation: Critical to Our Success

- 76% of appeals are closed before formal adjudication
- Successful resolution, through early resolution and/or mediation, saves significant time and resources for all parties
- The goal is to find a timely resolution that satisfies the interests of all involved

Adjudication

- When matters are not resolved at early resolution or through mediation, an appeal may proceed to adjudication
- Adjudication is a more formal inquiry process where any outstanding issues are examined and a decision, or order, is made
- The adjudication process begins with a “notice of inquiry” inviting written “representations”
- Non-confidential portion of parties’ representations are shared with the other parties
- The IPC may compel a party to produce documents or testimony
- After all representations are received and considered, the IPC may issue a binding order which is published

Privacy Obligations under FIPPA/MFIPPA

- FIPPA/MFIPPA protects the right of privacy through rules for the collection, use and disclosure of personal information by an institution

- Institutions cannot collect personal information, unless:
  - Authorized by a statute
  - Used for law enforcement
  - Necessary for a lawfully authorized activity

Privacy Obligations under FIPPA/MFIPPA

Institutions cannot use personal information unless permitted under legislation, including for instance:

- For the purpose collected
- For a consistent purpose
- With consent

Institutions cannot disclose personal information unless permitted under legislation, including for instance:

- With consent
- For a consistent purpose
- To comply with legislation
- For law enforcement
- Health or safety
- Compassionate reasons

Privacy Obligations under FIPPA/MFIPPA

- Institutions shall ensure that reasonable safeguarding measures are in place to protect records in their custody or under their control from unauthorized access or from inadvertent destruction or damage

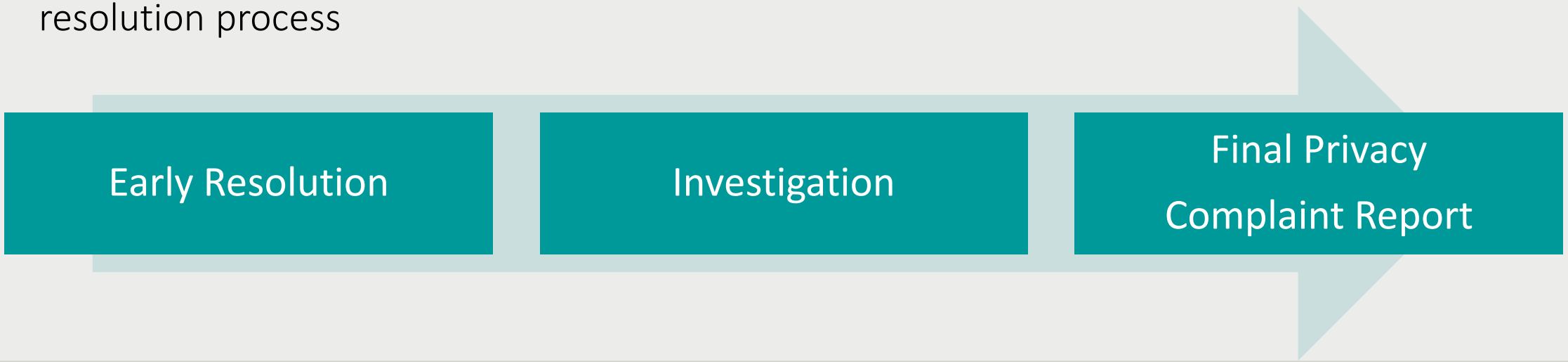
- Institutions shall also take reasonable steps to ensure that personal information held by the institution is not used unless it is accurate and up to date, and must retain it for at least one year to ensure that the individual to whom it relates has a reasonable chance to obtain access to it

Privacy Complaint Process

- A person who believes their privacy rights have been infringed by an institution may file a complaint with the IPC

- Although not mandatory, institutions may also report data breaches to the IPC. For example, where a breach involves sensitive personal information, large numbers of individuals, or when there are difficulties containing the breach

- Privacy complaints and reported breaches may also go through our Tribunal dispute resolution process



Personal Health Information Protection Act (PHIPA)

PHIPA applies to personal health information in the custody or control of health information custodians, such as health practitioners, hospitals, pharmacies, laboratories, long-term care homes etc.

The purpose of PHIPA is to:

- protect the confidentiality of personal health information (PHI) in the custody or control of health information custodians
- provide individuals with a right of access to, and correction of, their own PHI, subject to limited and specific exemptions

A number of duties are imposed on health information custodians and their agents, including:

- collection, use and disclosure of PHI
- responding to requests for access and correction
- security of personal health information
- transparency of information practices
- duty to report breaches to affected individuals, and to the IPC

Cont'd

PHIPA

- The IPC is the oversight body for administering and enforcing PHIPA
- A person who has reasonable grounds to believe that another person has contravened or is about to contravene PHIPA may make a complaint to the Commissioner
- The Commissioner may also, on her own initiative, conduct a review of any matter if she has reasonable grounds to believe that a person has contravened or is about to contravene the Act or its regulations
- The Commissioner may investigate a matter, publish her report of findings and issue a binding order against the health information custodian
- Pending the adoption of regulations, the Commissioner can also issue administrative monetary penalties in serious cases where the circumstances warrant it

Health Privacy Breach Investigations

Early Resolution

- Breach not significant
- We are satisfied with steps taken to rectify the matter

Investigation/Mediation

- Investigate whether health information custodian has responded adequately
- File may be closed by a decision or mediator's report
- Where a complainant is involved, we attempt to find a consensual resolution
- If not resolved or closed, file sent to adjudication

Adjudication

- Review of facts
- If notice of review is issued, parties involved may provide further details
- Adjudicator will issue decision, may include orders and recommendations
- Possible follow-up to ensure compliance

Child, Youth and Family Services Act (Part X) (CYFSA)

- Part X of the CYFSA applies to records of personal information in the custody or control of a service provider, that are collected for the purpose of providing a service to children and youth, including:
  - Child protection services delivered by children's aid societies
  - Indigenous child and family services
  - Residential services, such as group homes and foster homes
  - Secure treatment
  - Youth justice
  - Adoption
- The paramount purpose of the CYFSA is to promote the best interests, protection and well-being of children
- The CYFSA recognizes that appropriate sharing of information to plan and provide services is essential for creating successful outcomes for children and families

Cont'd

CYFSA (Part X)

- Similar to PHIPA, Part X of the CYFSA sets out rules respecting
  - the collection, use and disclosure of personal information
  - the right of access to, and correction of, one's own personal information
  - the security of personal information
  - transparency of personal information practices
  - the duty of service providers to report data breaches to individuals and to the IPC
- The IPC is the oversight body for administering and enforcing Part X
- A person who has reasonable grounds to believe that another person has contravened or is about to contravene Part X may make a complaint to the Commissioner
- The Commissioner may also, on her own initiative, conduct a review of any matter if she has reasonable grounds to believe that a person has contravened or is about to contravene Part X or its regulations
- The Commissioner may investigate a matter, publish her report of findings and issue a binding order against the provider

Access and Privacy in the News

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
- Resolution calls on governments and stakeholders to 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

- Digital ID 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
- Digital ID systems must be secured from identity theft, fraud or other harms
- Governments, organizations must be held accountable for their use and subject to independent oversight


CTV NEWS
TORONTO
TORONTO | News
Many Ontario employers now need 'electronic monitoring' policies. Here's what that means
TATTLEWARE
CTV National News: Who's monitoring their workers?
Abby O'Brien
Follow | Contact
Share
Many Ontario companies will s… whether they're electronically…
In April, Ontario became the fir… transparency law, as part of the… requiring companies with 25 or… written policy clearly outlining… computers, cellphones, GPS sy… devices are being tracked, and…
Ontario employers now… how they electronically…
JORDAN OMSTEAD
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
NATIONAL POST
Full Comment
Vass Bednar: Your boss is watching you while you work
Electronic surveillance in the workplace is nothing new, but it is becoming more sophisticated and alarmingly common as we work remotely
Bednar, National Post
August 18, 2020 • 4 minute read • Join the conversation

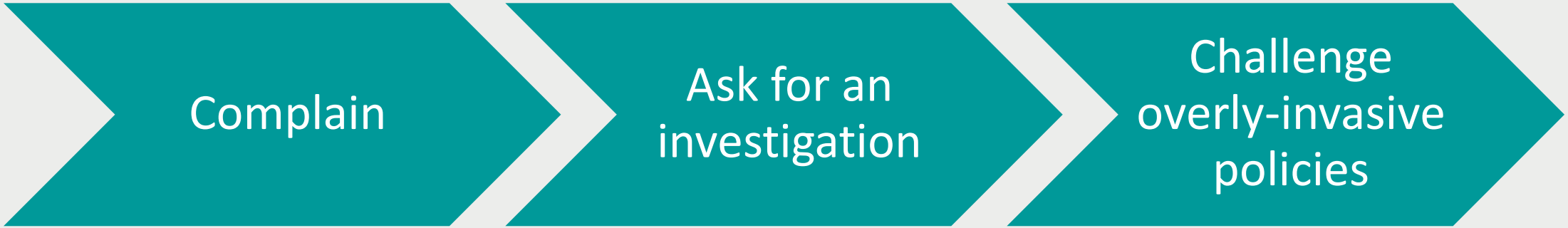
Bill 88, *Working for Workers Act, 2022*

- Introduced on February 28, 2022 and received Royal Assent on April 11, 2022.
- Amends the *Employment Standards Act* and 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 must be strengthened by allowing workers to do something with electronic monitoring policies.

- Workers should be able to:



Facial Recognition Technology

- Real time tracking or still image recognition
- Highly sensitive biometric data
- Ethical and legal issues
- Accuracy and reliability issues
- Scope creep

- Federal, provincial, and territorial privacy authorities issued a joint statement and guidance on the use of facial recognition technology (FRT) by law enforcement in May 2022
- IPC sponsored a resolution on principles and expectations for the use of personal information in FRT at 2022 Global Privacy Assembly

Consultation and Outreach

Work with MPPs and the Legislature

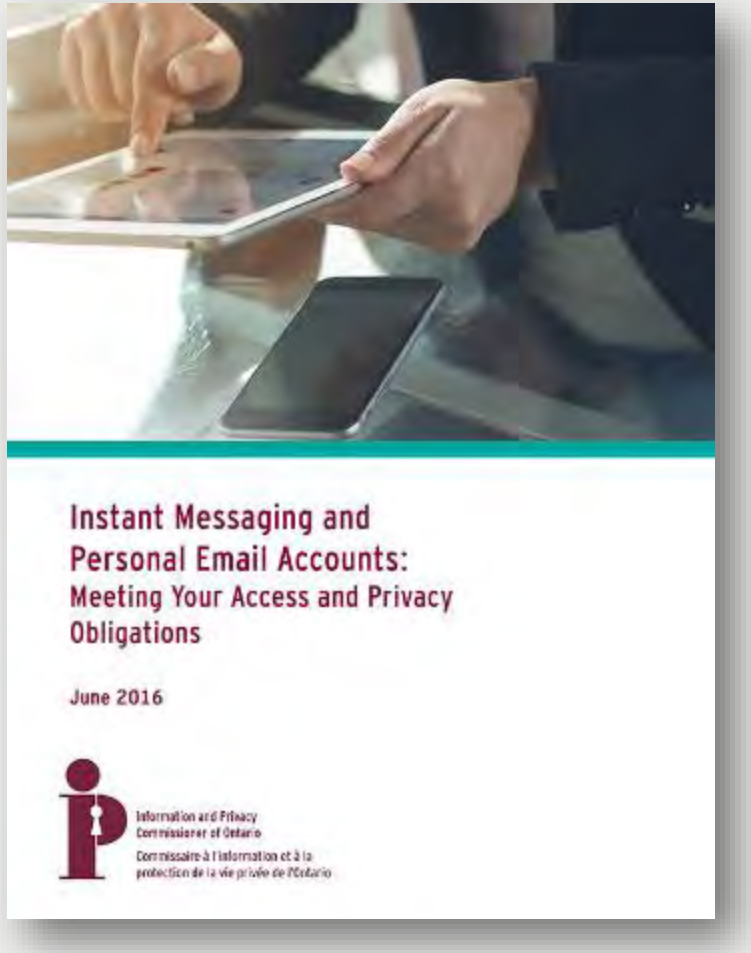
- As part of its statutory powers and duties, the IPC may offer comment on the privacy protection implications of proposed legislative schemes or government programs
- As recent examples, the IPC has been consulted on:
  - Ontario's white paper on Modernizing Privacy in Ontario
  - Amendments to the *Personal Health Information Protection Act* (*PHIPA*)
  - Policy framework for Ontario's digital identity program
  - Ontario's Trustworthy Artificial Intelligence (AI) Framework
  - Ontario's proposal for a new provincial data authority
  - COVID Alert app and Verify Ontario app
  - Ontario Health Data Platform
  - Strategy to combat human trafficking
  - Part X of the *Child, Youth and Family Services Act*

IPC Publications

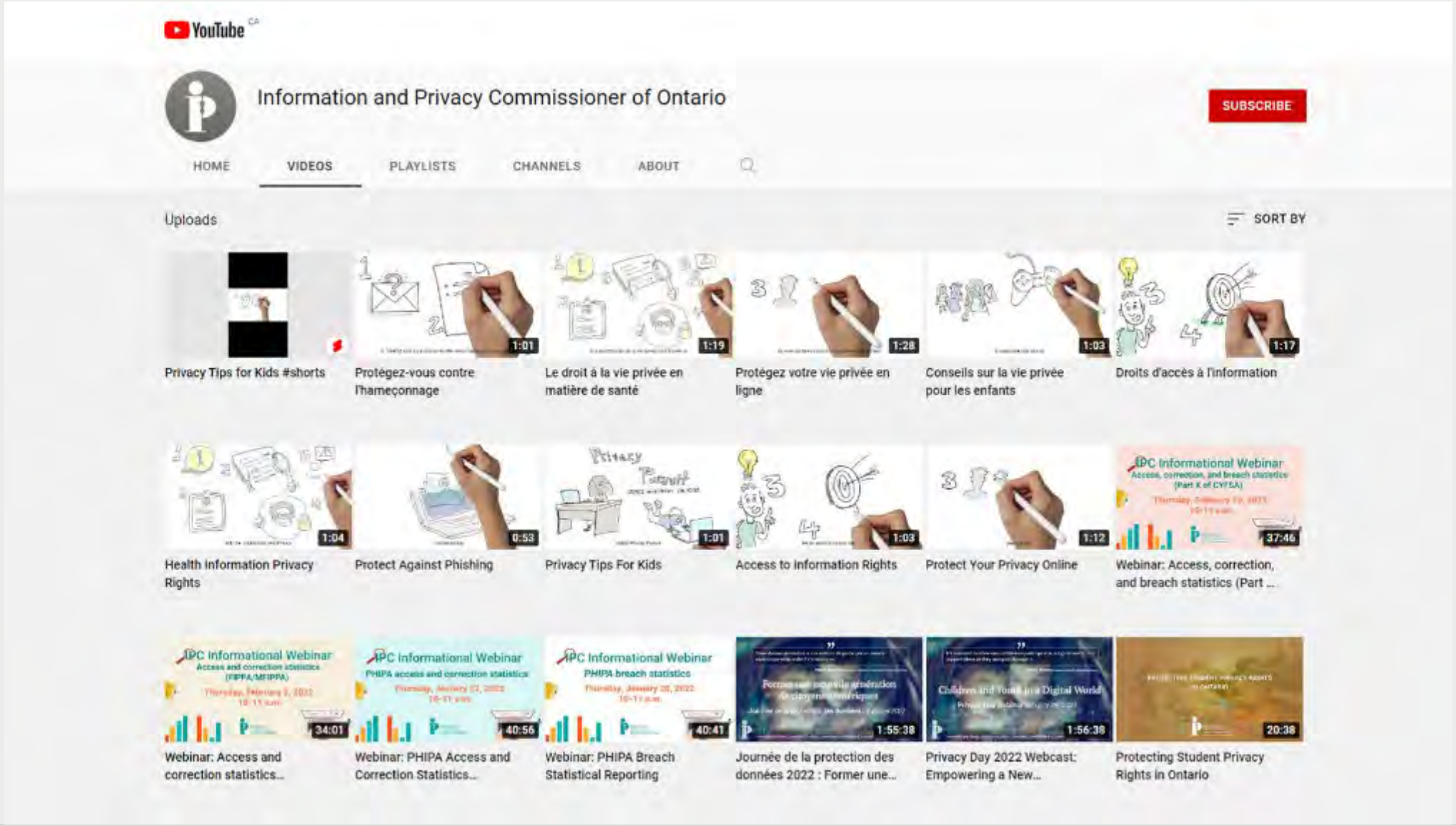
Visit www.ipc.on.ca for more

Instant Messaging and Personal Email Accounts

- Records relating to governments business that are created, sent or received through instant messaging or personal email accounts, are subject to the privacy and access provisions of FIPPA and MFIPPA
- The use of these tools creates significant challenges for compliance with the acts and recordkeeping requirements
- As a best practice, the IPC recommends that institutions and government prohibit the use of instant messaging or personal email accounts when conducting government-related business



IPC Videos and Webinars



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...

Info Matters

Information and Privacy Commissioner of Ontario

Government

★★★★★ 5.0 • 5 Ratings

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

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

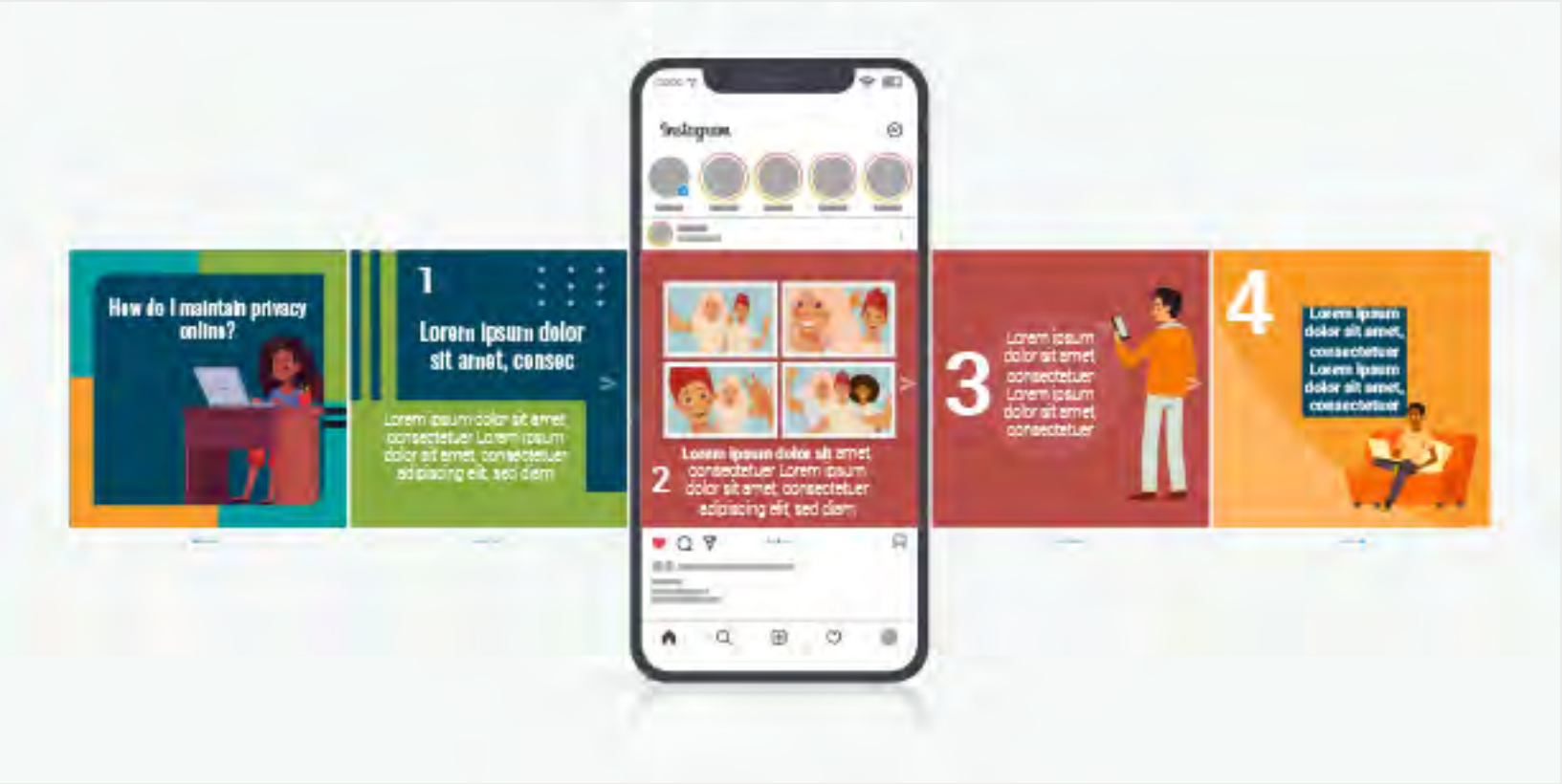
Data is the engine of the modern economy, a key driver of innovation and growth. While the power of data is undeniable, questions emerge about the impact of digital transformation on our human rights, our collective well-being, and the state of our democracy. Commissioner Kosseim speaks with Jim...

PLAY 29 min

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

Cont'd

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