Policing, Privacy and Public Trust

Stephen McCammon & Jesse Campbell

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

Tech Driven Community Safety 4th Annual COCPA Conference

October 3, 2024

Overview

This session will explore:

- Ontario's privacy legislation and the role of the Information and Privacy Commissioner of Ontario
- Privacy and transparency best practices for police when considering the adoption of new technologies
- Key examples of the IPC's work in its Next-Generation Law Enforcement Strategic Priority area and associated resources
- Consulting with the IPC

Disclaimer

This presentation should not be relied on as legal advice or as a substitute for the applicable legislation itself. It is not an official legal interpretation of the relevant law, nor does it bind the office of the Information and Privacy Commissioner of Ontario.

Key takeaways for today

- Police use of new technologies can bring significant benefits but can also raise concerns associated with police-community relations, the right to privacy, and what it means to live in a free and democratic society.
- The IPC's strategic priorities include contributing to building public trust in law enforcement by working with relevant partners to develop the necessary guardrails for the adoption of new technologies … that protect both public safety and Ontarians' access and privacy rights.
- IPC guidance can help police map out a plan to demonstrate their commitment to privacy, transparency and accountability in their use of technology, and support and sustain public trust.

Information and Privacy Commissioner of Ontario

Patricia Kosseim

Ontario's Information and Privacy Commissioner (IPC) is an officer of the legislature

- Appointed by and reports to the Legislative Assembly of Ontario
- Independent of the government of the day

The IPC has authority under the following laws:

- *Freedom of Information and Protection of Privacy Act*
- *Municipal Freedom of Information and Protection of Privacy Act*
- *Personal Health Information Protection Act, 2004*
- *Child, Youth and Family Services Act, 2017*
- *Anti-Racism Act, 2017*
- *Coroners Act*

IPC Role and Mandate

In addition to providing independent oversight of provincial access and privacy laws, the office of the IPC serves the Legislature, public institutions and other regulated entities, and the public through its mandate to:

- Resolve appeals when access to information is refused
- Investigate privacy complaints related to personal information
- Ensure compliance with the province's access and privacy laws
- Provide general guidance and best practices about privacy, security, and access issues and recommend improvements to current practices
- Conduct research on access and privacy issues and provide comment on proposed legislation and government programs
- Hear from and educate the public, media and other stakeholders about Ontario's access and privacy laws and current issues affecting access and privacy

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 institutions, 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)***
  - Applies to designated organizations authorized to collect personal information for the purpose of eliminating systemic racism and advancing racial equity under the *ARA*

Ontario privacy legislation – the broad strokes

- Institutions, service providers and HICs must :
  - follow rules governing how they collect, use, retain, disclose and dispose of personal information (and personal health information under PHIPA)
  - collect, use or disclose personal information only for legitimate, limited and specific purposes
  - inform individuals how they intend to use their information and how they can learn more
- Individuals have the right to:
  - request access to their own personal information
  - file privacy complaints
  - request access to any information held by institutions
  - appeal access requests and privacy complaint decisions to the IPC

Looking ahead - Bill 194

- If passed, Bill 194 - the ***Strengthening Cyber Security and Building Trust in the Public Sector Act*, 2024** - will establish cyber security and artificial intelligence system requirements for public sector entities, and introduce new privacy protections and strengthen oversight under FIPPA, including by:

i. Requiring institutions to conduct PIAs prior to the collection of PI;

ii. Requiring institutions to take reasonable steps to protect personal information;

iii. Requiring institutions to report privacy breaches to the IPC; and

iv. Providing the IPC with new powers to review, investigate and issue orders in relation to privacy breaches.

- The IPC has urged the government to hasten its plans to introduce equivalent changes to MFIPPA.

Bill 194 and artificial intelligence

- FIPPA and MFIPPA institutions subject to the Bill 194 **artificial intelligence** regime will be required to:
  - Provide information to the public regarding their use of prescribed AI systems.
  - Develop and implement an accountability framework regarding their use of those systems.
  - Take steps to manage risks associated with their use of those AI systems.
  - Comply with prescribed restrictions and prohibitions on the use of artificial intelligence systems.

IPC Vision of a Modern and Effective Regulator

APRIL 2021

IPC Strategic Priorities 2021–2025

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

Privacy and Transparency in a Modern Government

Advance Ontarians' privacy and access rights by working with public institutions to develop bedrock principles and comprehensive governance frameworks for the responsible and accountable deployment of digital technologies.

Trust in Digital Health

Promote confidence in the digital health care system by guiding custodians to respect the privacy and access rights of Ontarians, and supporting the pioneering use of personal health information for research and analytics to the extent it serves the public good.

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.

Next-Generation Law Enforcement

Contribute to building public trust in law enforcement by working with relevant partners to develop the necessary guardrails for the adoption of new technologies and community based approaches that protect both public safety and Ontarians' access and privacy rights.

Accessibility & Equity

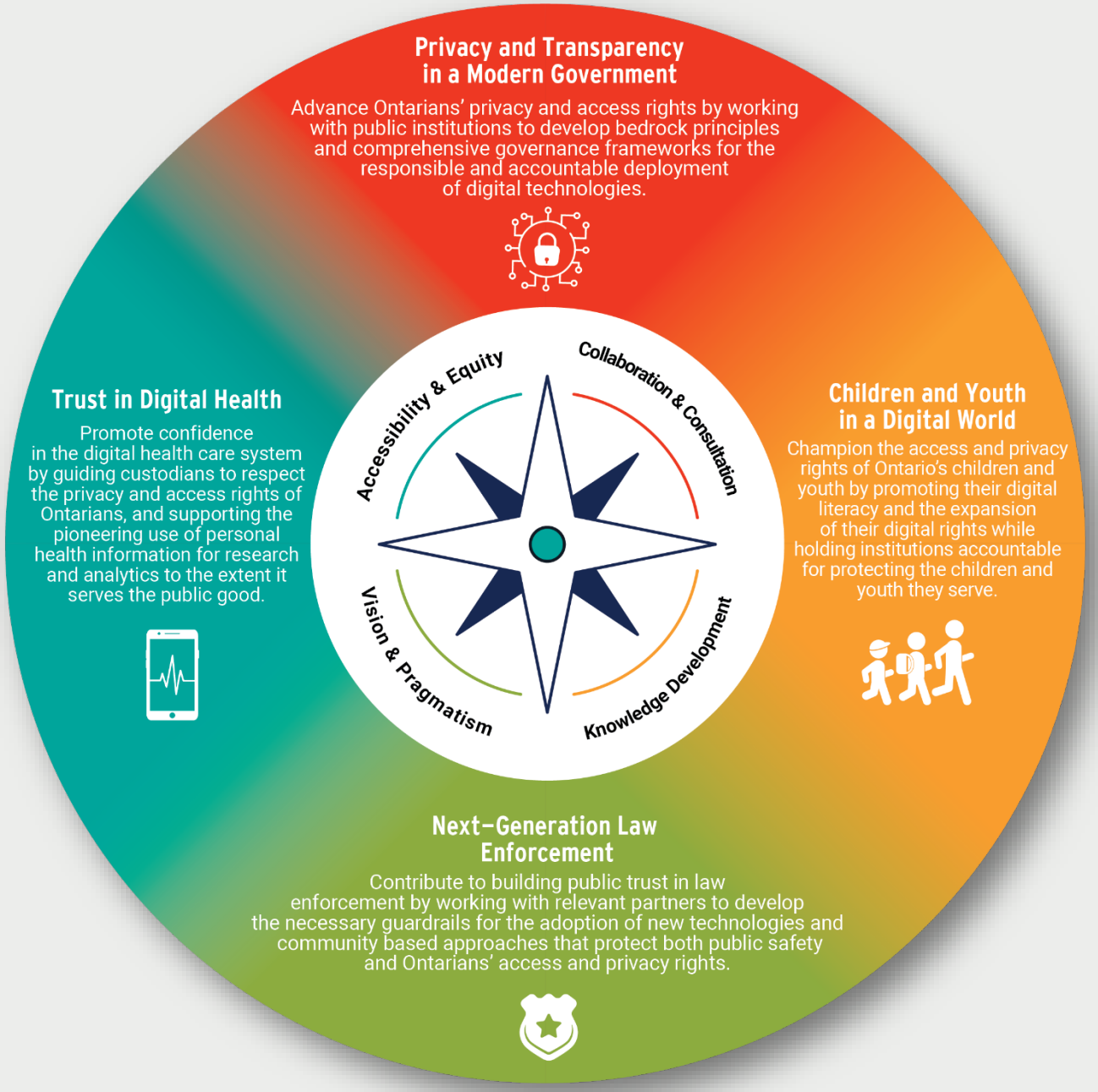
Collaboration & Consultation

Vision & Pragmatism

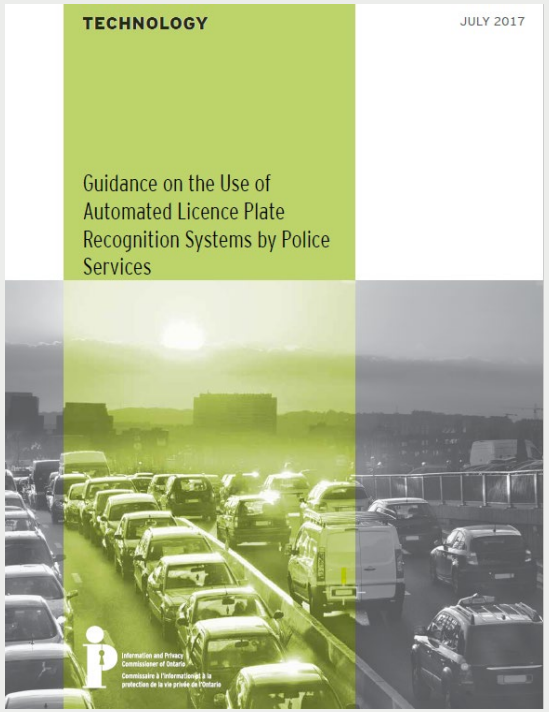
Knowledge Development

Next-Generation Law Enforcement

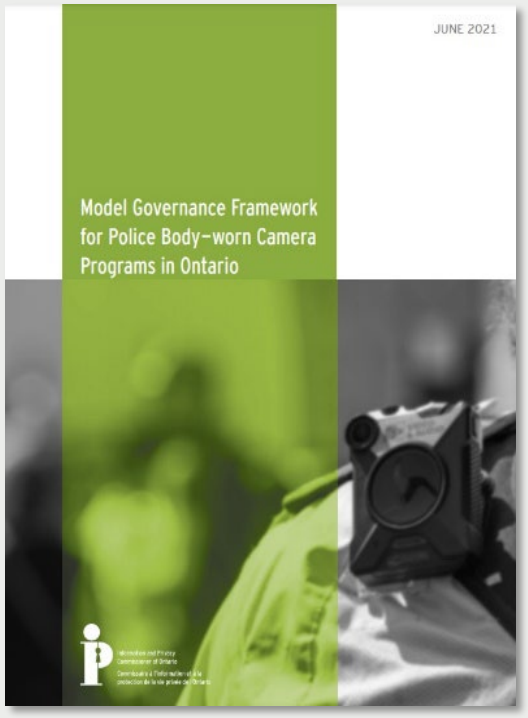
Contribute to building public trust in law enforcement by working with relevant partners to develop the necessary guardrails for the adoption of new technologies and community-based approaches that protect both public safety and Ontarians' access and privacy rights.



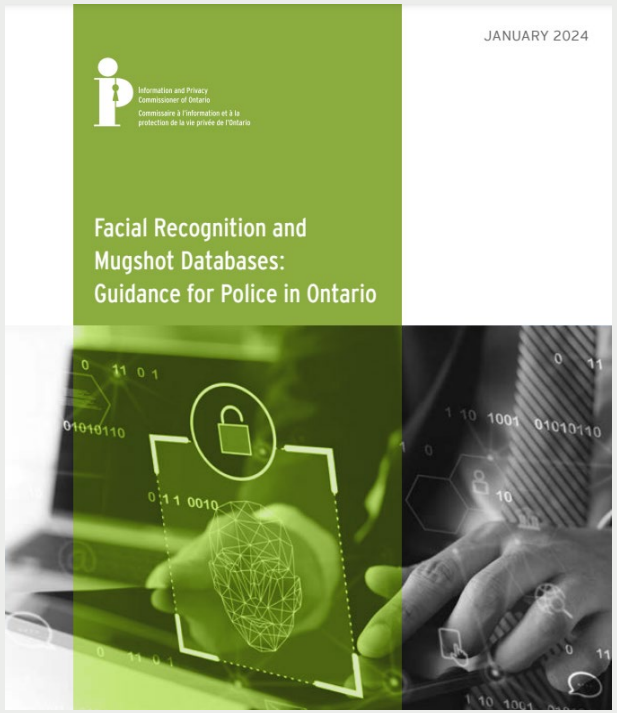
IPC Guidance for Police Services



Automated Licence Plate Recognition Systems



Body-worn Cameras



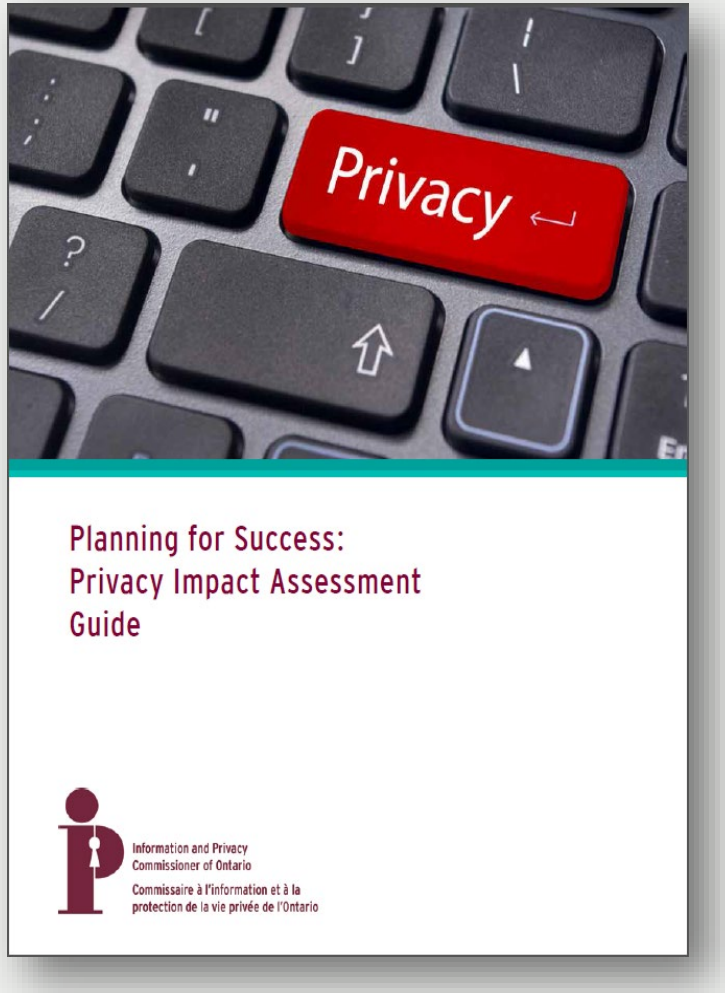
Facial Recognition Technologies

Tips and best practices for implementing new technology programs

Planning for Success: Privacy Impact Assessments

- PIAs are tools to identify **privacy impacts** and **risk mitigation strategies**
- Widely recognized as a **privacy best practice** across Canada and globally
- IPC developed a PIA Guide which includes a simplified **4 step methodology** and tools for M/FIPPA institutions

www.ipc.on.ca/en/resources-and-decisions/planning-success-privacy-impact-assessment-guide



Practical tips for conducting a PIA

1. Start your PIA early and have the hard convos right away
2. Consult with affected parties and privacy experts
3. Involve the right people and build expertise in-house
4. Don’t treat it as a check box activity
5. Thoroughness is necessary to ensure risks are identified and mitigated
6. Adapt the PIA process to suit the needs of the project and your organization
7. Ensure the PIA report can be understood by non-technical audiences
8. Designate who is responsible for approvals and managing residual risks
9. Treat the PIA as evergreen – updates will be required if significant changes to the program are planned
10. Consider how you will share the findings of your PIA with affected parties to improve transparency and public trust

Privacy and transparency tips and best practices

When novel or high-risk technologies are being contemplated, police services are encouraged to:

- Conduct a PIA process that leverages individuals with critical expertise
- Consult with the IPC, relevant external experts, affected parties, and the public, including individuals from Indigenous, racialized, and other marginalized communities
- Develop guiding principles that take into consideration the broader privacy and human rights risks and societal implications
- Conduct a pilot program prior to full scale implementation
- Be transparent with the public by making plain-language information about the program available to the public, including by posting your PIA report or an informative summary of it and governance documents on your website
- Conduct regular periodic reviews and audits of the program as part of your commitment to ensuring that your tech programs are necessary, proportional and minimally intrusive

Privacy and public trust is built on:

- **Strong governance** to ensure the organization is in a position to fulfill their privacy-related responsibilities
- **Training, policies, procedures and practices are in place** to ensure staff and the organization continues adherence to privacy requirements and best practices
- **Strong safeguards:** taking steps to ensure that personal information is appropriately protected against inappropriate access, use or disclosure
- **Transparency:** being open with the public about the adoption of new technologies and how they will be used and governed, before and after deployment

Next-Generation Law Enforcement Engagement

Examples of IPC - Police Use of Tech Consultations

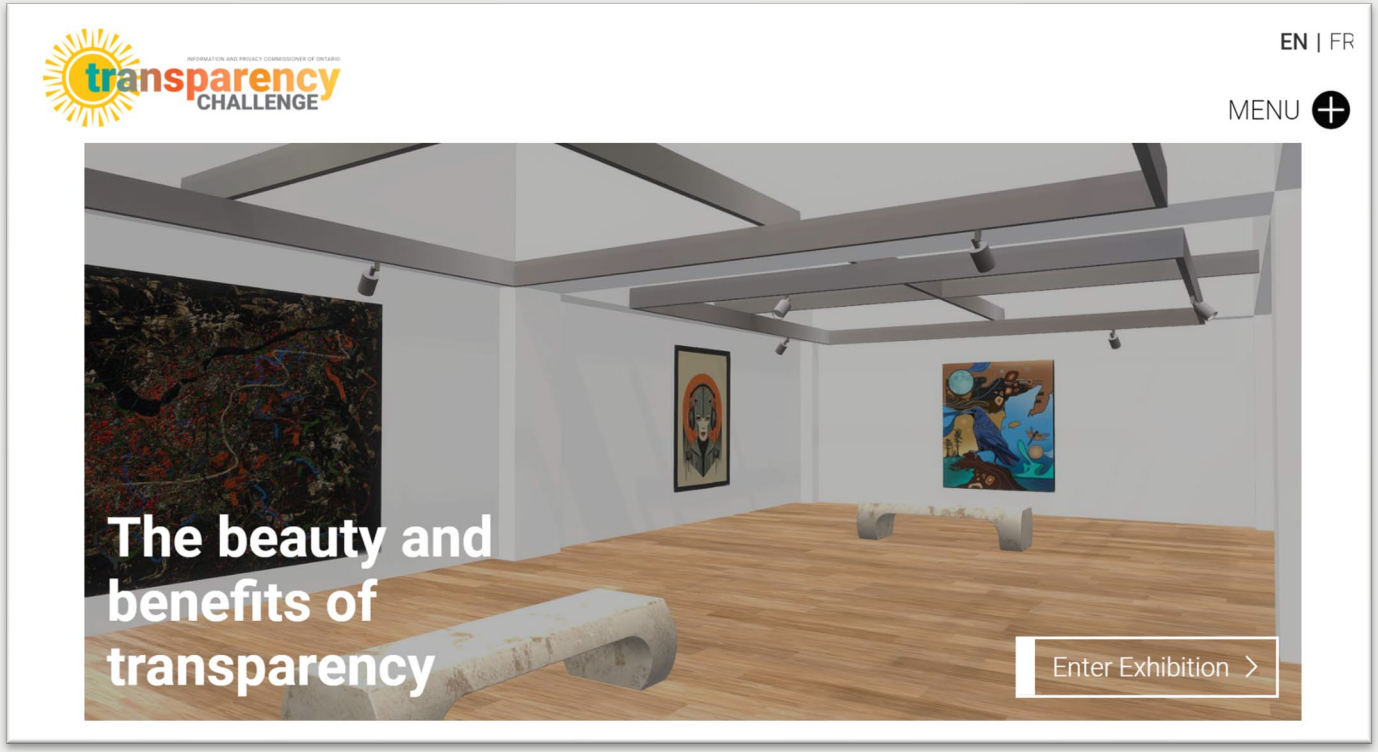
- 2015 Annual Report
  - *Ontario Provincial Police*: Automatic License Plate Recognition Program
  - *Toronto Police Service*: Pilot project on the use of Body-Worn Cameras
- 2016 Annual Report
  - *Toronto Police Service*: Open Data Strategy
- 2017 Annual Report
  - *Durham Regional Police Service*: Body Worn Camera Pilot Project
  - *Niagara Regional Police Service*: Crime Mapping Tool
- 2018 Annual Report
  - *Toronto Police Service*: Full body scanner pilot project
  - *Waterloo Regional Police Service:* Unmanned aerial vehicles privacy impact assessment
- 2019 Annual Report
  - *Peel Regional Police and York Regional Police:* Facial recognition technology

Examples of IPC - Police Use of Tech Consultations

- 2020 Annual Report
  - *Peel Regional Police*: Real Time Operations Centre
  - *Sault Ste. Marie Police Service:* Fixed Camera Automated License Plate Recognition System
  - *Toronto Police Service Board and Service*: Body-Worn Camera Governance Framework
- 2021 Annual Report
  - *St. Thomas Police Service*: Body-Worn Cameras
  - *Waterloo Regional Police Service*: New Policing Technologies, including GrayKey and BriefCam
- 2022 Annual Report
  - *Thunder Bay Police Service*: Use of a Technology to Rapidly Review Surveillance Footage
  - *Toronto Police Service Board and Service*: AI Technology Policy, Procedure and Pre-Assessment Screening Form
- 2023 Annual Report
  - *Ottawa Police Service*: Community Safety Data Portal
  - *Sault Ste. Marie Police Service*: Downtown CCTV
  - *Thunder Bay Police Service*: Draft Use of Artificial Intelligence Policy

The IPC's Transparency Showcase 2.0

- Innovative projects that support government transparency, civic engagement, and demonstrate the positive impact of open data for Ontarians
- 30+ projects featured from Ontario's public institutions, including, provincial ministries, municipalities, schools, universities, and police services
- Provide inspiring models for other institutions to follow



https://transparencyshowcase.ipc.on.ca

Consulting with the IPC

Policy consultations with the IPC

- Our proactive policy work involves consultations with public institutions and others about new programs, projects, technologies and processes
- We can offer comments, provide guidance and suggest best practices about privacy, security, and access issues
- IPC consultations do not provide legal advice or endorse or approve programs or certify that your activities comply with privacy and access laws

How to prepare for a consultation with the IPC

Before you reach out to the IPC for a consultation, we generally recommend you:

- Are past the initial ideation, research or discovery stage of your project
- Have engaged your internal privacy, policy and legal experts in initial discussions
- Have conducted a PIA or have a draft PIA underway
- Can describe the kinds of data/personal information that will be involved in the project
- Have identified the Legal Authority you will be relying on to collect personal information
- Are aware of the potential privacy/security impacts of your project
- Are clear about your objectives for consulting with our office
- Review our **Consultations FAQs** https://www.ipc.on.ca/about-us/policy-consultations/

➢ **To request a consultation, contact policy.consultations@ipc.on.ca**

Concluding words

- Properly understood, access and privacy legislation helps discipline rather than prevent the effective delivery of vital public services
- When used effectively, PIAs help to ensure that programs meet legal requirements and mitigate privacy risks
- With novel or high-risk technologies, police services should consult relevant experts and affected parties early on and before deployment
- Police services should monitor and re-assess privacy risks, and the effectiveness of privacy protections on an ongoing basis
- Respecting privacy and being transparent are essential to ensuring sustainable public trust in service delivery

Questions?

HOW TO CONTACT US

Information and Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073

TDD/TTY: 416-325-7539

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

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