

Privacy Law Backgrounder

Brian Beamish

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

Osgoode Hall Law School

Toronto, Canada

September 20, 2019

What is Privacy?

Personal privacy

- Right to be left alone or not intruded upon
 - Who controls this?
- Bodily privacy
 - physical searches (ex. airport pat-down)
 - medical testing (urine, genetic, blood)
- Property (your home)

What is Privacy?

Informational privacy

- Collection, use, disclosure, retention, access to your own information
 - Who controls this? (e.g., smart cities)
- Emails, texts, online behavior – privacy is an evolving target
- What is publicly available and what is not?
- Group privacy?

Jurisdictional Attitudes Towards Public's Right to Know

American vs. Canadian expectations about public disclosure of politicians' health status





Privacy, what privacy?

“When top earners’ tax returns are published in Finland, they call it “national envy day”. In Sweden, one phone call will get you your lawmaker’s tax bill. Norwegians’ fascination with each others’ taxes has been labeled “financial porn”.

“Many Nordic tax records are a phone call away”, Reuters, April 12, 2016

Comparative Approaches to Privacy Regulation

Comprehensive

- Rules and obligations on collection, use, disclosure of personal information in
 - public sector
 - private sector
- Authority or regulator provides oversight

Sectoral

- Law addresses specific industries (credit records, websites aimed at children, medical records, marketing)
- May be more than one authority or regulator (for each industry)
- Enforcement may also be through private civil actions

Privacy Law in Canada - Federal



- *Privacy Act* – public sector privacy legislation
- *Personal Information Protection and Electronic Documents Act* – private sector privacy laws, including access
- *Anti-Spam Act* – sending of commercial electronic messages to electronic address, altering transmission data and installation of a computer program

Provincial Overview - IPC's Mandate

- *Freedom of Information and Protection of Privacy Act (FIPPA)*
 - covers 300 provincial institutions
- *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*
 - covers 1,200 municipal organizations
- *Personal Health Information Protection Act (PHIPA)*
 - covers individuals and organizations involved in the delivery of health care services
- Expanded Mandate: *Child, Youth and Family Services Act* (January 1, 2020)

Our Office

- IPC provides **independent** review of government decisions and practices on access and privacy
- Commissioner appointed by, reports to the Legislative Assembly, to ensure **impartiality**
- 125 staff
 - Tribunal
 - Policy
 - Health Policy
 - Legal
 - Communications
 - Corporate Services & IT

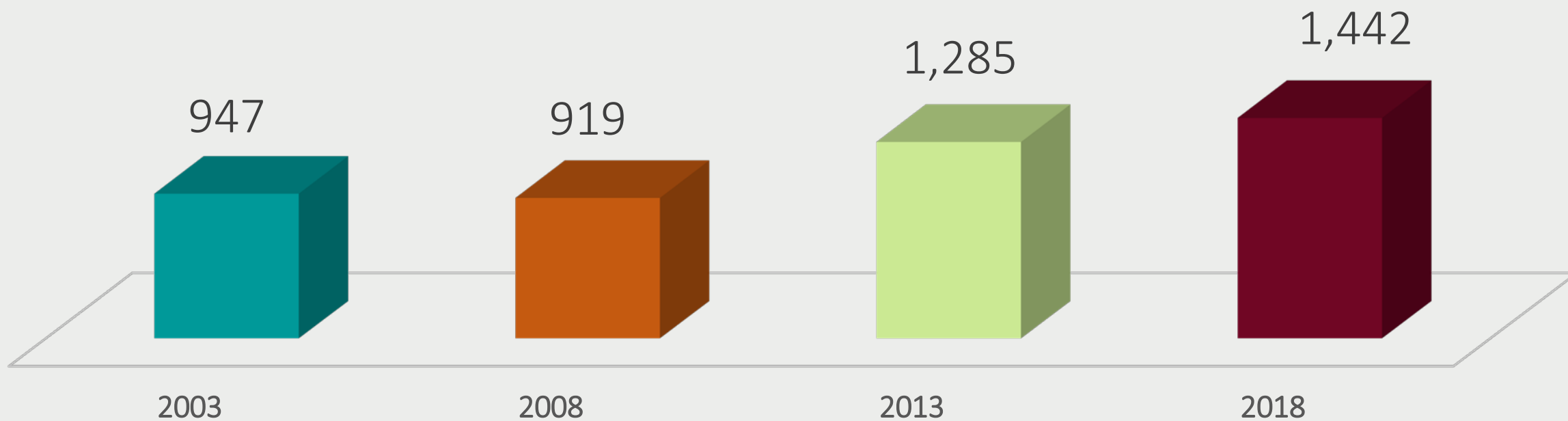


FOI and Democracy

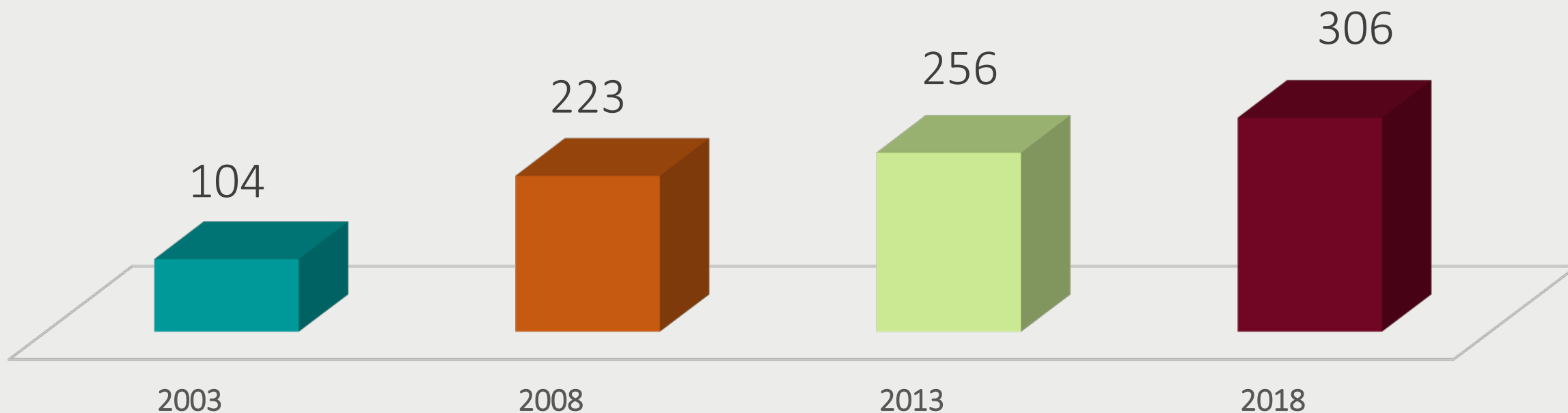
“We do not now and never will accept the proposition that the business of the public is none of the public’s business.”

- Attorney General, Ian Scott, 1987

Appeals Received Per Year



Total Privacy Complaints Opened Per Year



What Smart Cities May Offer

A community that uses connected technologies to collect and analyze data to improve services for citizens:

- less congestion and traffic accidents
- increased safety for cyclists and pedestrians
- better environment
- efficient use of public resources
- better informed citizens



Keep in Mind

- Smart City issue far more than Sidewalk Toronto
- These are CITIES
- The private sector needs to realize that involvement with public sector changes the rules

Privacy Risks of Smart Cities

- Privacy not barrier to smart cities, but they require strong **privacy protections**
- Without adequate safeguards, excessive **personal information** may be collected, used, disclosed
- Potential hazards:
 - tracking individuals as they go about their daily activities (**surveillance**)
 - use/disclosure for other purposes without consent (**function creep**)
 - security breaches (**cyberattacks**)

Annual Report Recommendation

- *MFIPPA* is outdated in the face of current digital technologies and practices
- Government should lead a comprehensive review of our privacy laws and modernize them to address the risks inherent in smart city technologies
- Areas of concern:
 - need for proper oversight and enforcement
 - address public/private partnerships
 - data trust?

2018

ANNUAL REPORT

Office of the Information
and Privacy Commissioner
of Ontario

Privacy and Accountability for a Digital Ontario



Data Analytics

- Changing how we think about, use data
- New combinations of data may reveal hidden patterns and insights
- Data integration (sharing, linking, analyzing data) can enhance:
 - policy development
 - system planning
 - resource allocation
 - performance monitoring

Privacy Risks of Data Integration

- Not consent-based, lack of transparency
- Multiple massive government databases of PI
- Surveillance and profiling of individuals
- Increased cybersecurity risks
- Potential discrimination based on inaccurate data/flawed algorithms

Budget Bill Amends *FIPPA*

- Schedule 31 of 2019 budget bill amends *FIPPA* to include Part III.1 (Data Integration)
- Part III.1 sets out privacy-protective framework to enable data integration:
 - designated units within ministries may indirectly collect PI from service providers and funded agencies
 - special “inter-ministerial” units may collect from other ministries
 - units may link PI but must then de-identify
 - responsible minister to establish data standards approved by IPC
 - IPC may conduct reviews of units, new **order-making powers**

Fixed Cameras for Law Enforcement

- Video surveillance can enhance public safety but must respect privacy laws
- Police can collect information using video surveillance if:
 - collection furthers a law enforcement purpose
 - surveillance is justified
- Examples:
 - video cameras for high crime areas
 - temporary cameras for special events (e.g., Pan Am Games)



Body-Worn Cameras

- Continuous recording collects more information than necessary for the law enforcement purpose
- Microphones capture ambient sound, including the conversations of bystanders
- Used inside private homes, increases the likelihood individuals will be recorded in highly personal situations



Facial Recognition

- When used with video surveillance, people can be identified and tracked in **real time**

Accuracy/reliability issues:

- poor quality images in the watch list database or flawed algorithms for making matches
- lighting, pose, facial features (i.e. aging), obstructions (i.e., glasses, hair, make-up) and image resolution

Scope creep:

- police using driver's licence or passport photo databases



The Philadelphia Model

- Review of police sexual assault files to look for deficiencies and biases
- Since implementation in Philadelphia 17 years ago, “unfounded rape” rate dropped to four per cent
- U.S. national average is seven per cent



Globe and Mail Series: *Unfounded*
Robyn Doolittle

MOU for Use by Ontario Police

- IPC worked with police and stakeholders to develop model Memorandum of Understanding and Confidentiality Agreement
- Sets the terms for the review of sexual assault cases by police and external reviewers
- Kingston Police are first to put into practice

MEMORANDUM OF UNDERSTANDING respecting the External Sexual Assault Case Review Program made this 1st day of November, 2017 (the "Effective Date").

BETWEEN:

SEXUAL ASSAULT CENTRE KINGSTON
(Hereinafter referred to as "SACK")

-AND-

PAMELA CROSS, BA, LLB
(Hereinafter referred to as "Pamela Cross")

-AND-

OTTAWA RAPE CRISIS CENTRE
(Hereinafter referred to as "ORCC")

COLLECTIVELY REFERRED TO AS THE "KINGSTON VAW ADVOCACY GROUPS"

-AND-

KINGSTON POLICE
(Hereinafter referred to as "Kingston Police")

COLLECTIVELY REFERRED TO AS THE "PARTIES"

WHEREAS the Kingston Police as a municipal police service are governed by the *Police Services Act*, R.S.O. 1990, c. P. 15 (*PSA*) and the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M. 56 (*MFIPPA*);

WHEREAS, under section 1 of the *PSA*, police services shall be provided in accordance with principles, including the need for co-operation between the providers of police services and the communities they serve; the importance of respect for victims of crime and understanding of their needs; the need for sensitivity to the pluralistic, multiracial and multicultural character of Ontario society; and the need to ensure that police forces are representative of the communities they serve;

WHEREAS, under section 4(2) of the *PSA*, core police services include crime prevention, law enforcement, and providing assistance to victims of crime;

WHEREAS, under section 41(1) of the *PSA*, the duties of the Chief of the Kingston Police include ensuring that the Kingston Police provide community-oriented police services and that its members carry out their duties in a manner that reflects the needs of the community;

WHEREAS the duties and functions of the Kingston Police include investigating reports of sexual assault and supervising and monitoring those investigations, including for the purpose of identifying deficiencies, errors and anomalies in and improving the efficiency of individual sexual assault investigations and the sexual assault investigative process as a whole;

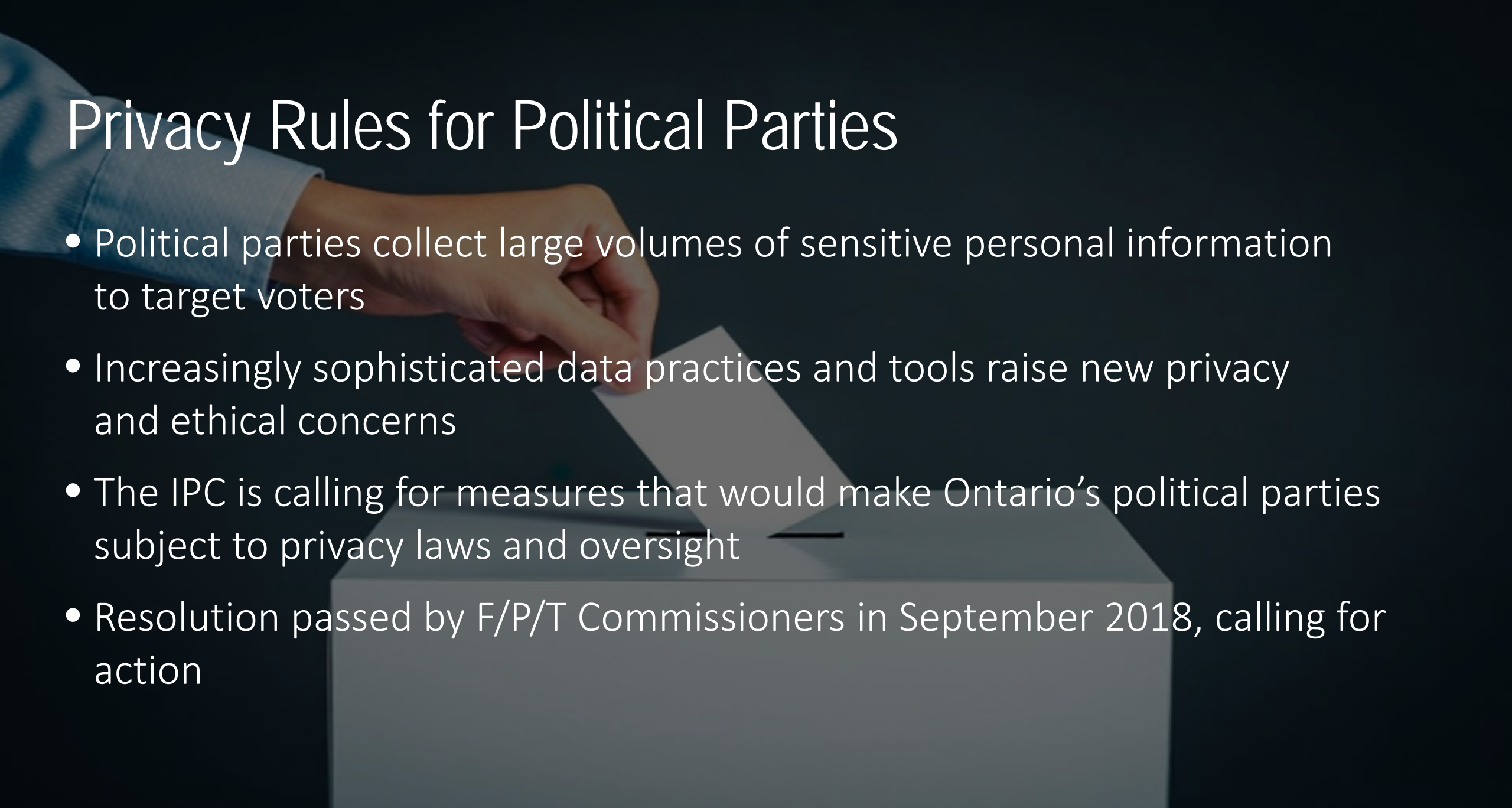
Supreme Court of Canada and Voyeurism

- High school teacher secretly recorded his female students' chests with a camera pen while they were engaged in normal activities at school
- Jarvis charged with voyeurism [*Criminal Code*, s. 162(1)(c)]
- Offence where person **(i) surreptitiously** observes/records another person in situation where **(ii) reasonable expectation of privacy**, if observation/recording for **(iii) sexual purpose**
- Jarvis acquitted at trial: students had reasonable expectation of privacy, but videos not for sexual purpose

Video Surveillance: Voyeurism

- Ontario Court of Appeal dismissed Crown's appeal; three judges say sexual purpose, but 2-1 majority says students **did not have a reasonable expectation of privacy** [acquittal]
- Supreme Court of Canada finds students did have reasonable expectation of privacy, all elements satisfied, Jarvis **convicted** [*R. v. Jarvis*, 2019 SCC 10]
- IPC intervened before SCC
- “Privacy is **not an all-or-nothing concept** ... being in a public or semi-public space does not automatically negate all expectations of privacy with respect to observation or recording” [Wagner C.J., para 41]

Privacy Rules for Political Parties

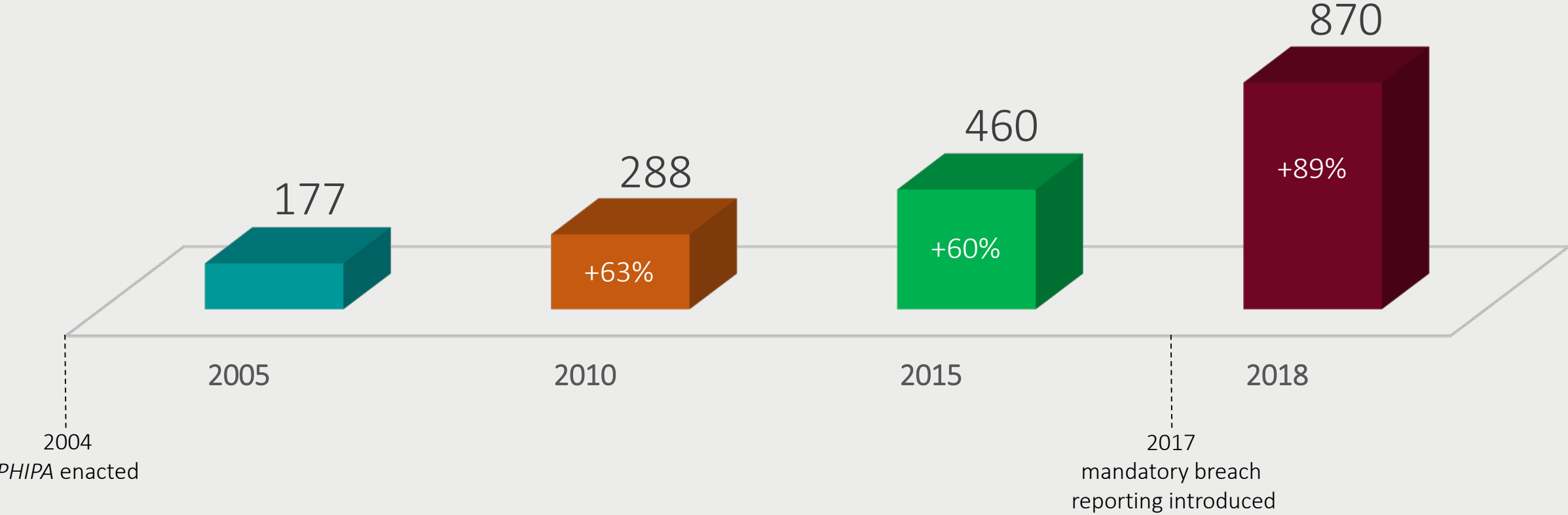
A hand in a blue shirt sleeve is shown dropping a white ballot into a grey ballot box. The background is dark, and the lighting is focused on the hand and the box.

- Political parties collect large volumes of sensitive personal information to target voters
- Increasingly sophisticated data practices and tools raise new privacy and ethical concerns
- The IPC is calling for measures that would make Ontario's political parties subject to privacy laws and oversight
- Resolution passed by F/P/T Commissioners in September 2018, calling for action



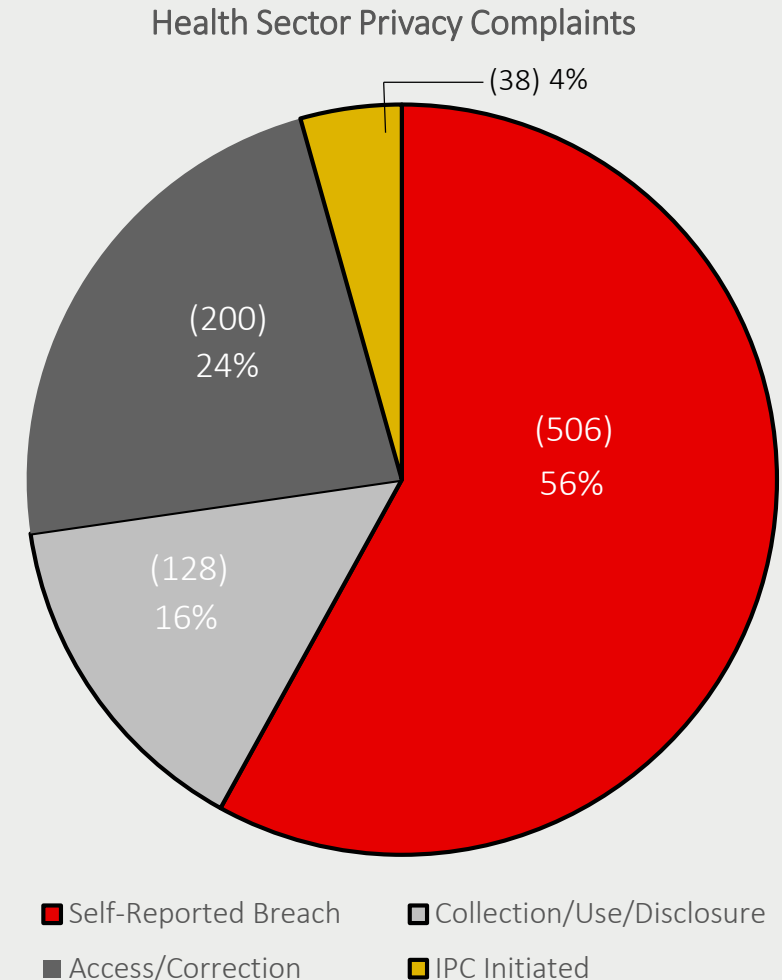
Health Privacy

PHIPA Complaints Opened per Year



Health Sector Privacy Complaints 2018

- Of the 506 self-reported breaches in 2018:
 - 120 were snooping incidents
 - 15 were ransomware/cyberattack
- Remaining 371 were related to:
 - lost or stolen PHI
 - misdirected information
 - records not properly secured
 - other collection, use and disclosure issues



Snooping – A Persistent Problem

- ***PHIPA* Decision 64** - A hospital registration clerk viewed the health records of a media-attracting patient and 443 other patients without authorization
 - the breach was discovered by the hospital during a proactive audit and reported to the IPC
 - the clerk was fired from the hospital and pled guilty to breaking Ontario's health privacy law
- The IPC concluded:
 - the employee had used personal information in contravention of *PHIPA*
 - the hospital had sufficient safeguards in place

Prosecutions

To date, five individuals have been successfully prosecuted:

- **2016** – two radiation therapists at a Toronto Hospital
- **2016** – a registration clerk at a regional hospital
- **2017** – a social worker at a family health team*
- **2017** – an administrative support clerk at a Toronto hospital

*The fine in this case is the highest fine to date for a health privacy breach in Canada - the social worker was ordered to pay a \$20,000 fine plus a \$5,000 victim surcharge.

Fighting “Snooping” – Innovative Audit Solution

- Project to address the challenge of auditing transactions
- Use data analytics and AI
- IPC was approached by Mackenzie Health to participate in the project steering committee and provide a regulatory perspective
- Other partners included Michael Garron Hospital, Markham Stouffville Hospital and vendor, KI design
- Our office provided input throughout the pilot, particularly on the project objectives and assessment criteria



- CBC Marketplace investigation reveals Toronto plastic surgeon, Dr. Gix, may have been filming patients in states of undress without their consent
- Surveillance camera discovered in a consultation room
- He is now under investigation by both College of Physicians and Surgeons of Ontario and the IPC

MARKETPLACE

'It's creepy': Security cameras spotted in plastic surgeon's consult room



Marketplace investigation sparks probes by Ontario privacy commissioner and College of Physicians and Surgeons

Caitlin Taylor, Makda Ghebreslassie - CBC News -

Posted: Dec 14, 2018 4:00 AM ET | Last Updated: December 14, 2018



A teal background with a large, semi-transparent green speech bubble on the left side. The word "Resources" is written in white inside the speech bubble.

Resources

Privacy Fact Sheet: Disclosure of Personal Information to Law Enforcement

- When can institutions disclose personal information to a law enforcement agency?
 - when legally required
 - to aid a law enforcement investigation
 - for health or safety reasons
- Disclosing institutions need to:
 - document disclosure requests and court orders
 - be transparent about their decisions
 - develop and publish policies about how they make and document decisions about disclosure

Disclosure of Personal Information to Law Enforcement

Under Ontario's access and privacy laws, institutions are prohibited from disclosing personal information, except in defined situations.

This fact sheet describes the key situations where institutions (public sector organizations such as provincial ministries and agencies, municipalities, schools, transit systems) can disclose personal information to a law enforcement agency under the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act*. It also explains how to respond when a law enforcement agency requests personal information, and how to be transparent to the public about disclosure decisions.

Generally, institutions should disclose personal information to a law enforcement agency *only when required by law*, such as in response to a court order, rather than a simple request, where there is no requirement to disclose.

However, they have the discretion to disclose in other situations, including where disclosure is made to aid an investigation, and for health or safety reasons.

In all cases, an institution should make its own careful and informed assessment of the circumstances before deciding whether to disclose personal information to a law enforcement agency. If uncertain, it should seek legal advice.

REACHING OUT TO ONTARIO

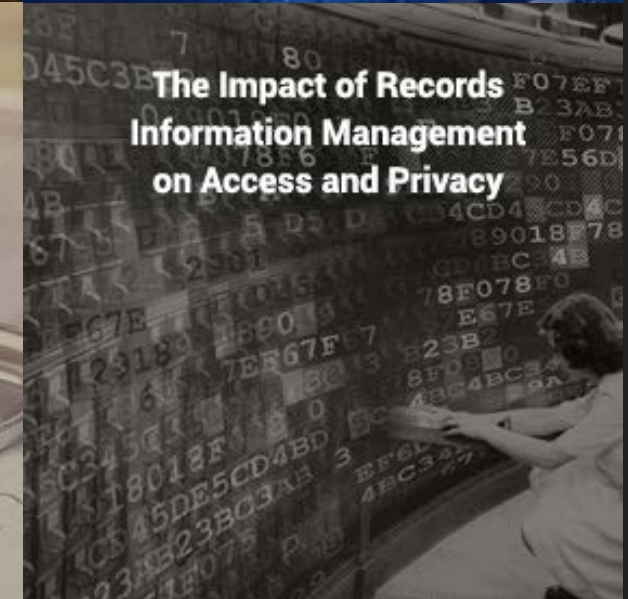
ROTO is an ongoing program where we visit communities across Ontario and host events to discuss the latest developments in access and privacy with stakeholders and the public



- St. Catharines
- Ottawa
- Sault Ste. Marie
- Kingston
- Barrie
- London
- Thunder Bay
- Windsor
- Hamilton
- Waterloo

IPC Webinars

- The webinar series has helped us to overcome geographical barriers and engage with Ontarians, regardless of where they live or work
- Registrants watch a live presentation and participate in a QA session
- Past webinar presentations on our website



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