

# Freedom of Information and Privacy at the IPC

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

WeirFoulds

November 29, 2018

# Our Office

- Information and Privacy Commissioner (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
  - Legal
  - Communications

# IPC's Mandate

- *Freedom of Information and Protection of Privacy Act (FIPPA)*
- *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*
- *Personal Health Information Protection Act (PHIPA)*

## Expanded mandate:

- *Child, Youth and Family Services Act*
- *Anti-Racism Act*



## 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

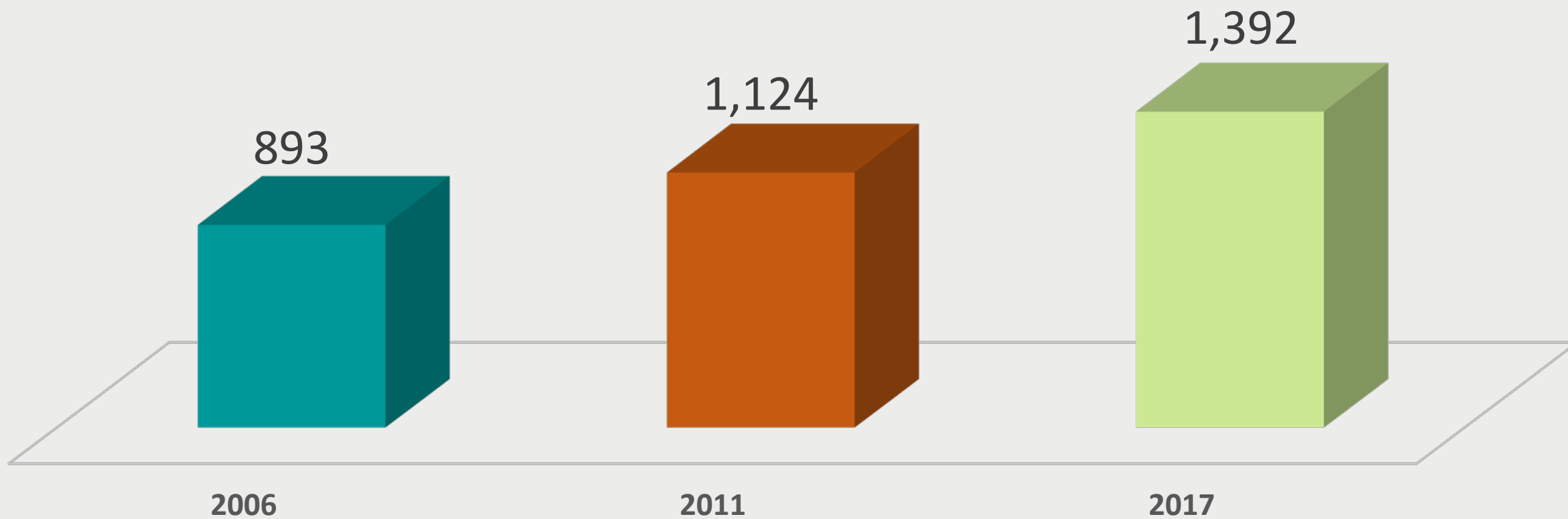


## Privacy in the Internet Age

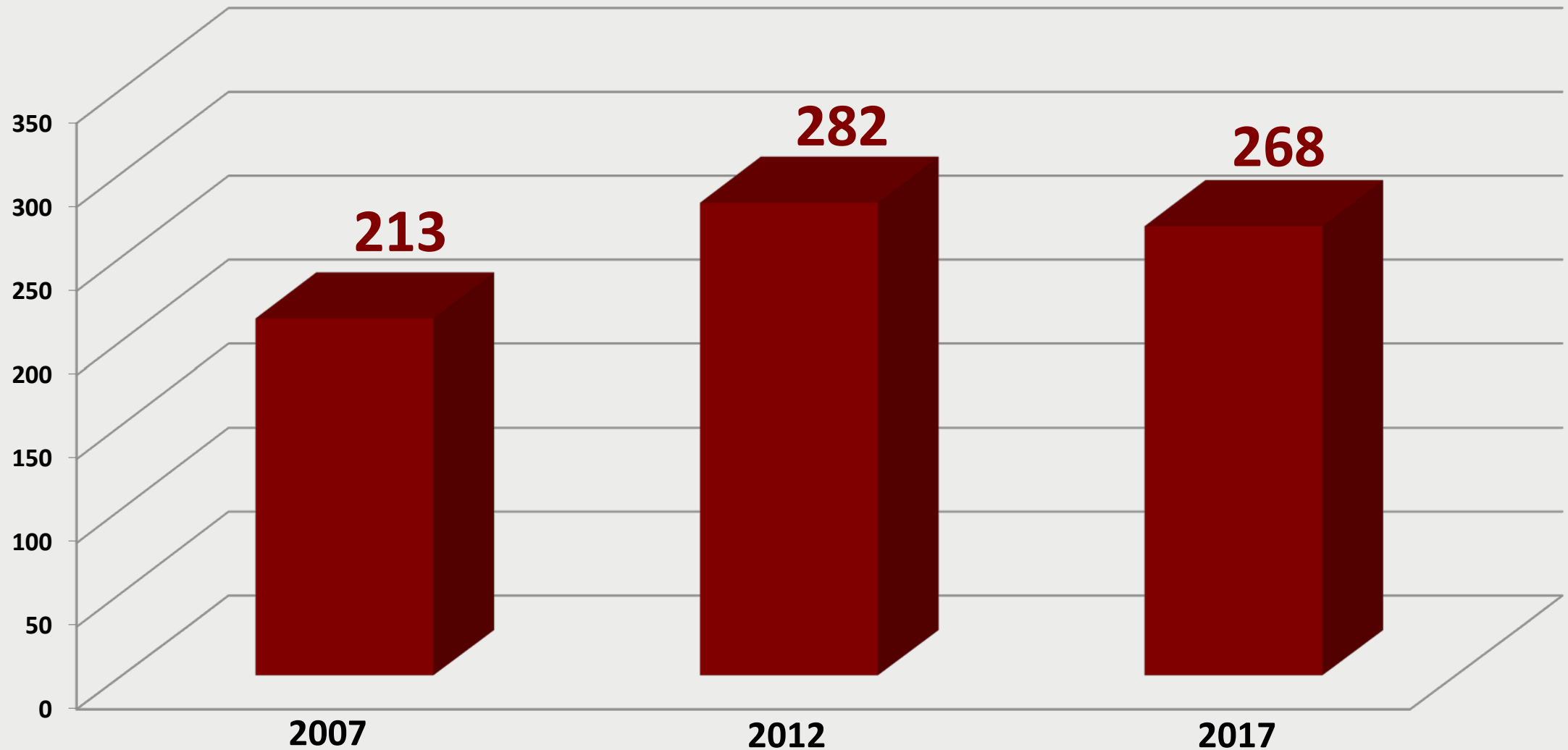
“Privacy legislation has been accorded quasi-constitutional status (Lavigne). This Court has emphasized the importance of privacy – and its role in protecting one’s physical and moral autonomy – on multiple occasions...the growth of the Internet, virtually timeless with pervasive reach, has exacerbated the potential harm that may flow from incursions to a person’s privacy interest...”

Supreme Court of Canada (Doez v. Facebook, 2017)

# Appeals Received per Year



# Total Privacy Complaints Opened Per Year



# Smart Cities

- A community that uses connected technologies to collect and analyze data to improve services for citizens
  - energy conservation sensors that dim streetlights when not in use
  - parking apps that indicate nearest available public parking spot
  - garbage cans that send a signal when full





# Privacy Risks

- Privacy is not a barrier to smart cities, but they require robust **privacy protections**
- Without safeguards in place, large amounts of **personal information** may be collected, used, disclosed
- Potential hazards:
  - tracking individuals as they go about their daily activities (**surveillance**)
  - using information for other purposes without consent (**scope creep**)
  - security breaches (**cyberattacks**)



# Minimize Privacy Risks

- Strong safeguards can protect personal information
  - privacy impact and threat/risk assessments
  - data minimization
  - de-identified data
  - encryption
  - privacy and access governance
  - contracts with private sector partners that address ownership of data
  - community engagement and project transparency
- IPC is working with municipalities and federal government
  - encourage transparency
  - ensure that privacy protections are built into smart city initiatives



# Surveillance Technologies

- IPC supports use of surveillance technologies to enhance community safety and deter unlawful activity, providing they are implemented in a manner that protects privacy
- Privacy implications associated with surveillance technologies include:
  - Potential to collect large amounts of personal information about individual users, including who they communicate with and what they communicate about
  - Ability to track the locations of individuals over time and to facilitate profiling of law-abiding individuals going about their everyday activities

# 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)



# Sudbury's "Eye in the Sky"

- For many years, the Sudbury Police have operated the "Lions' Eye in the Sky" program, using cameras on downtown streets live-monitored by volunteers
- A recent expansion of the program led the IPC to review the program to ensure it complied with privacy law
- IPC decided the program and the expansion were justified
- Our policy department worked with the police to make sure the details of the surveillance complied with privacy best practices

# 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



# City of Hamilton CCTV and Private Properties



VIA ELECTRONIC MAIL

February 13, 2018

Fred Eisenberger  
Mayor  
City of Hamilton  
Hamilton City Hall  
2<sup>nd</sup> Floor, 71 Main Street West  
Hamilton, ON L8P 4Y5

Eric Girt  
Police Chief  
Hamilton Police Service  
155 King William Street  
Box 1060, LCD1  
Hamilton, ON L8N 4C1

Dear Mayor Eisenberger and Chief Girt:

**Re: CCTV cameras and private properties**

I am writing to you about a significant privacy issue involving the City of Hamilton's proposed use of CCTV images taken by private individuals. Council's General Issues Committee passed a motion on February 7, 2018, that city staff work with the Hamilton Police Service to review the current CCTV by-law applicable to private homes and assess the feasibility of amending it to permit the collection of personal information from public spaces for use by the police.

As you know, my office oversees the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*, which applies to municipal government institutions and law enforcement agencies, and sets rules for protecting the privacy rights of Ontarians. The use of surveillance cameras by the city or police, and the collection of images from private cameras, must comply with this law.

In my view, any attempt by the city to permit or encourage the use of private video surveillance cameras, for the purpose of collecting personal information to aid in law enforcement, would undermine privacy rights under *MFIPPA*.

While in some cases CCTV surveillance may enhance public safety and the security of assets, it also poses risks to the privacy of individuals whose personal information may be collected, used and disclosed. The risk to privacy is particularly acute because video surveillance may, and often does, capture the personal information of law-abiding individuals going about their everyday activities. In view of the broad scope of personal information collected, special care must be



Tel: (416) 326-3333  
1 (800) 387-0073  
Fax/Télé: (416) 325-9195  
TTY: (416) 325-7539  
Web: www.ipc.on.ca

- Hamilton is reviewing CCTV by-law to assess feasibility of amendment to permit police to collect footage from security cameras of citizens
- Coverage is currently restricted to owner's property, amended by-law would enable broader coverage
- Hamilton is encouraged to leave the by-law un-amended

# 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





# Gunshot Locator Systems

- Detects location of gunfire to decrease response time

## Privacy protections

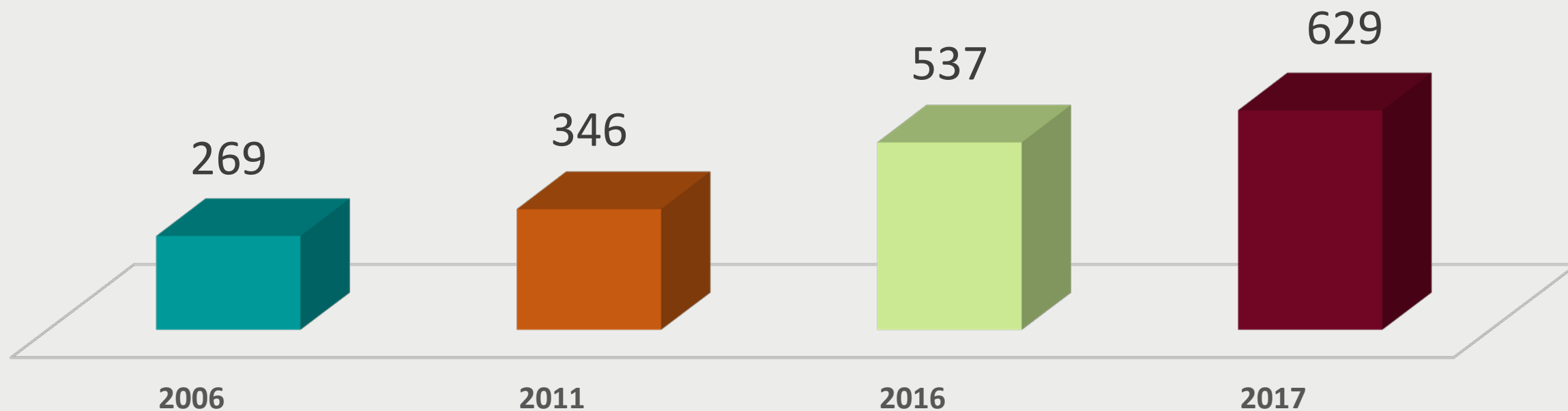
- position to avoid recording conversations
- overwrite audio recordings continually unless a gunshot is detected





Health Privacy

# PHIPA Complaints Opened per Year



# Mandatory *PHIPA* Breach Reporting

- As of October 1, 2017, health information custodians must notify IPC of certain privacy breaches
  - use or disclosure without authorization
  - stolen information
  - further use or disclosure
  - breaches occurring as part of a pattern
  - breaches related to a disciplinary action against a college or non-college member
  - significant breaches
- Custodians began collecting breach statistics in January 2018 for reporting in March 2019

## 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**.

As a custodian, you must report breaches to the Commissioner in seven categories described in the regulation and summarized below. The categories are not mutually exclusive; more than one can apply to a single privacy breach. If at least one of the situations applies, you must report it. The following is a summary—for the complete wording of the regulation, see the appendix at the end of this document.

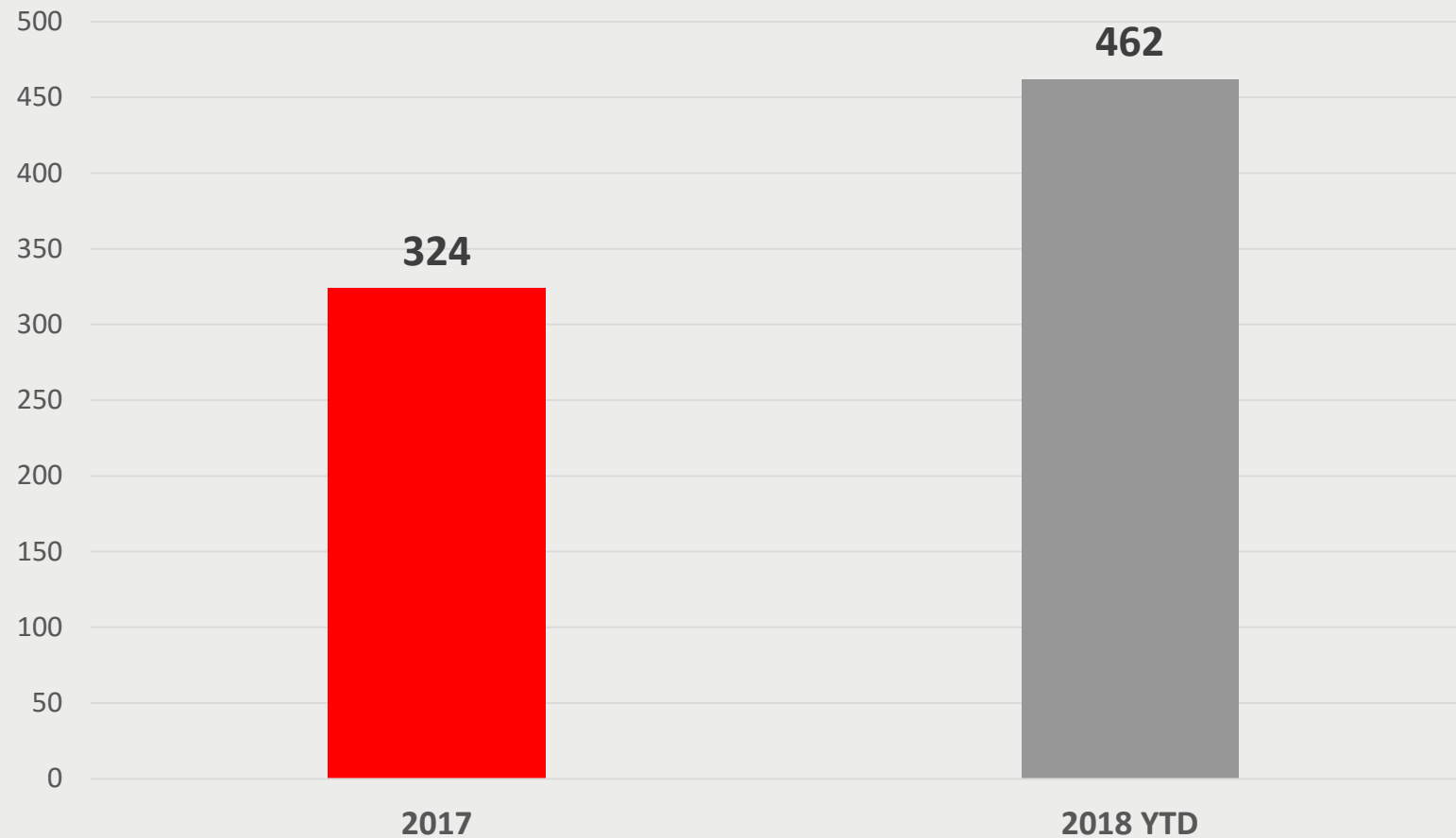
It is important to remember that even if you do not need to notify the Commissioner, you have a separate duty to notify individuals whose privacy has been breached under section 12(2) of the act.

### SITUATIONS WHERE YOU MUST NOTIFY THE COMMISSIONER OF A PRIVACY BREACH

#### 1. Use or disclosure without authority

This category covers situations where the person committing the breach knew or ought to have known that their actions are not permitted either by the act or the responsible custodian. An example would be where a

# Self-Reported Breaches Before and After Mandatory Breach Reporting



# Prosecutions

To date, six individuals have been prosecuted:

- 2011 – Nurse at North Bay Health Centre
- 2016 – Two radiation therapists at a Toronto Hospital
- 2016 – Registration clerk at a regional hospital
- 2017 – Social worker at a family health team
- 2017 – Administrative support clerk at a Toronto hospital

# Recent *PHIPA* Prosecution

- Administrative clerk in the emergency department of a GTA hospital
- Illegally accessed health records of 44 individuals, in some cases printing their personal health information
- October 2017 the clerk pleaded guilty and the court imposed a \$10,000 fine



Legislation



# *Child, Youth and Family Services Act*

- The *CYFSA* received Royal Assent on June 1, 2017
- Part X of the *CYFSA* was proclaimed along with the rest of the *CYFSA* on April 30, 2018, but will come into effect on January 1, 2020
- Part X of the *CYFSA* represents a big step forward for Ontario's child and youth sectors:
  - closes a legislative gap for access and privacy
  - promotes transparency and accountability

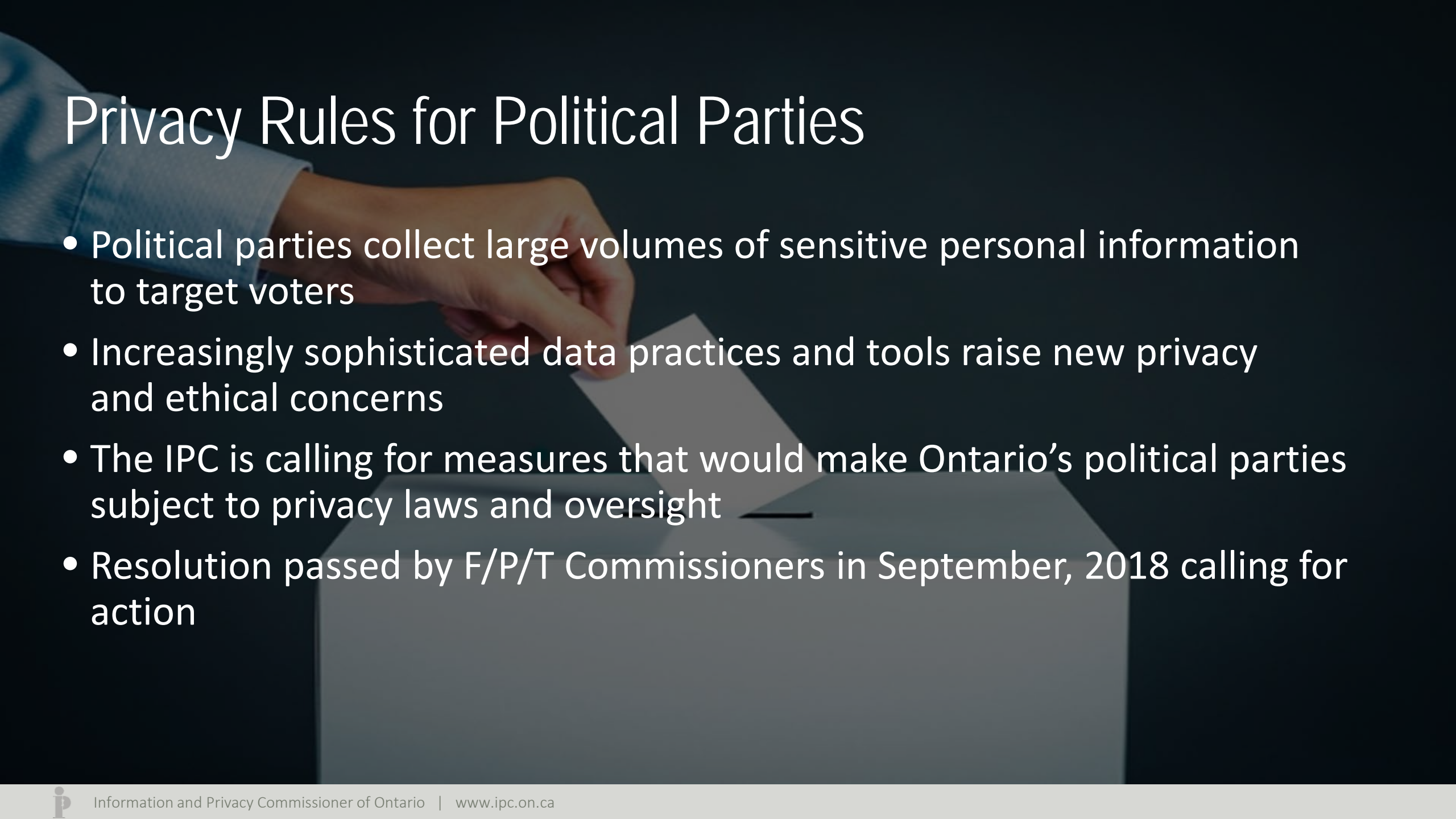
# Child, Youth and Family Services Act

- Strengths of Part X:
  - modelled after PHIPA
  - consent-based framework
  - individuals' right of access to their personal information
  - mandatory privacy breach reporting
  - clear offence provisions
  - adequate powers for the IPC to conduct reviews of complaints
  - facilitates transparency and consistency among CASs' information practices

# Child, Youth and Family Services Act

- Part X gives individuals the right to access:
  - records of their personal information (PI)
  - in a service provider's custody or control and
  - that relate to the provision of a service to the individual
- No fees can be charged for access except in prescribed circumstances (currently, none are prescribed)
- Appeal access decisions to IPC

# Privacy Rules for Political Parties

A hand in a blue shirt is shown dropping a white ballot into a grey ballot box. The background is dark, and the scene is lit from the side, creating a dramatic effect.

- 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



# Recent Court Activity

# OHIP Billings

"...the concept of transparency, and in particular, the closely related goal of accountability, requires the identification of parties who receive substantial payments from the public purse..."

IPC Order PO-3617

News · Queen's Park

## Ontario's top-billing doctor charged OHIP \$6.6M last year

Health minister flags 500 doctors who made more than \$1 million last year in a bid for public support in reforming outdated OHIP system.



# Reasonable Expectation of Privacy: *Jarvis* (SCC)

- High school teacher charged with voyeurism
- Using pen camera to surreptitiously record face and cleavage of 27 female students in common areas of school
- IPC intervened before Supreme Court of Canada on “reasonable expectation of privacy” in public spaces issue
- Crown/IPC say students in common areas have objective expectation of privacy, including in areas with existing video cameras
- Decision expected later in 2018

# Rouge Valley Health System – Order HO-013

- Hospital employees accessed records of personal health information of mothers who had recently given birth to market and sell RESPs
- The IPC found that the hospital did not take steps that were reasonable to safeguard personal health information
- This breach also led to at least one proposed class action
- The Ontario Securities Commission brought charges against hospital employees as well as RESP salespeople/dealers under the *Securities Act* and the *Criminal Code* which led to five guilty pleas

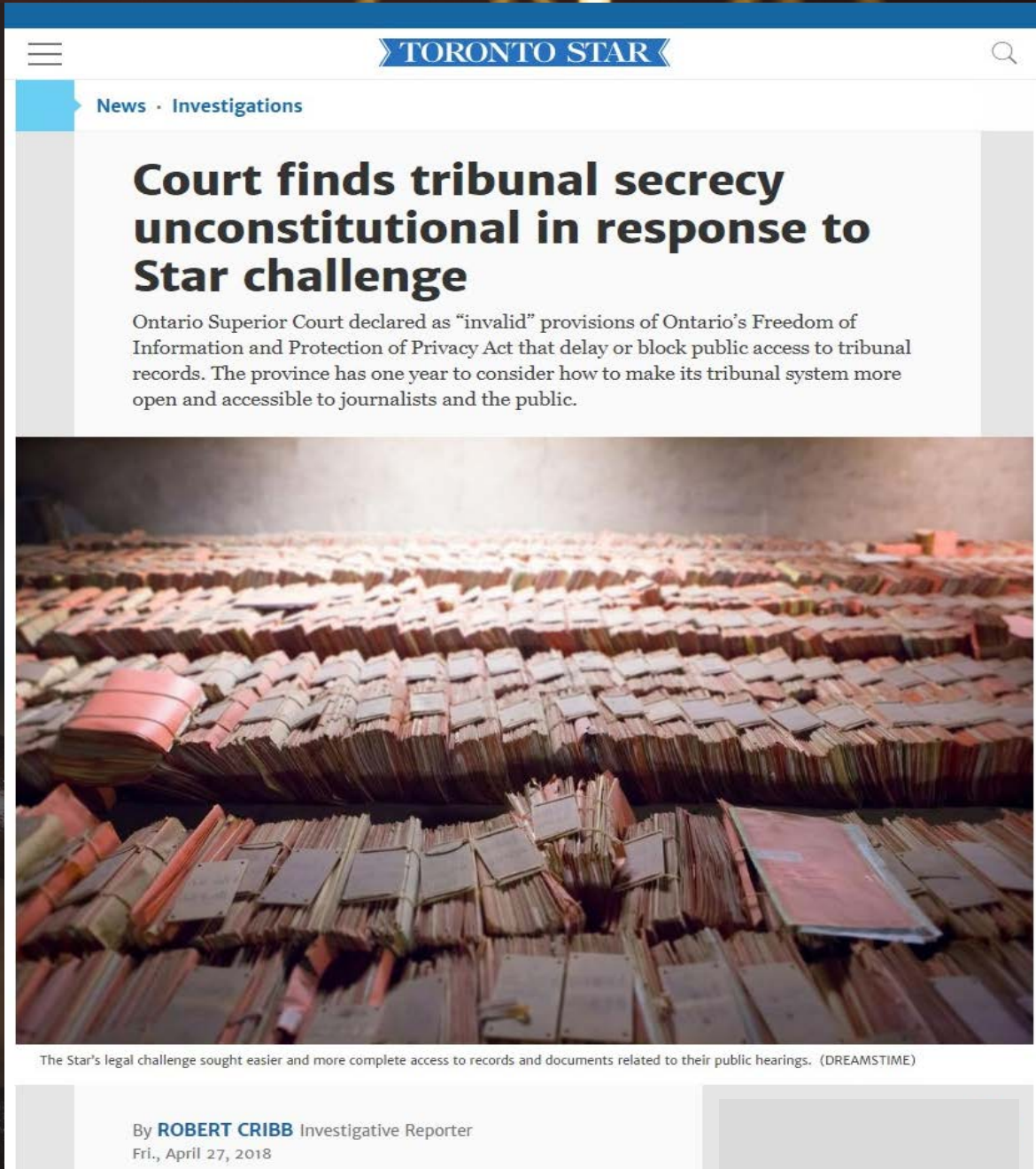


# *Broutzas v. Rouge Valley Health System, 2018 ONSC 6315*

- Proposed class actions were started because of privacy breaches at the Rouge Valley Health System and The Scarborough Hospital.
- In a recent decision, the Ontario Superior Court refused to certify two proposed class actions. Among other things, the Court held that:
  - a class action was not the preferable procedure for resolving these claims, and
  - a claim for “intrusion upon seclusion” could not succeed.

*“We strongly support the concepts of openness and transparency as applied to administrative tribunal hearings. If the government decides to move forward to amend the Freedom of Information and Protection of Privacy Act, we would be happy to work with them to find the right balance between openness of tribunals, and privacy and other confidentiality interests.”*

— IPC statement to the Toronto Star



The screenshot shows a news article from the Toronto Star. The page has a blue header with the 'TORONTO STAR' logo and a search icon. Below the header, there is a blue navigation bar with 'News · Investigations'. The main headline is 'Court finds tribunal secrecy unconstitutional in response to Star challenge'. Below the headline is a sub-headline: 'Ontario Superior Court declared as “invalid” provisions of Ontario’s Freedom of Information and Protection of Privacy Act that delay or block public access to tribunal records. The province has one year to consider how to make its tribunal system more open and accessible to journalists and the public.' The article is accompanied by a large photograph of numerous stacks of papers, some bound with red and orange bands, filling a room. At the bottom of the article, there is a byline: 'By ROBERT CRIBB Investigative Reporter Fri., April 27, 2018'. A small caption below the photo reads: 'The Star’s legal challenge sought easier and more complete access to records and documents related to their public hearings. (DREAMSTIME)'

# Public Interest

The public interest must be considered to ensure that privacy does not get in the way of the greater good.

# Public Sector Expense Disclosures

- **Sunshine List** - Publishing salary information for the highest paid public servants is important for accountability and transparency
- Proactive, on-line disclosures of travel and hospitality expenses of senior public servants

The screenshot shows the top of the Ontario government website. The header includes the Ontario logo, a search bar, and a menu button. The main heading is "Public sector salary disclosure". Below it, a paragraph explains that the site lists the names, positions, salaries, and total taxable benefits of public sector employees paid \$100,000 or more in a calendar year. A blue button labeled "Search the 2017 disclosure" is prominent. To the right, a "Related" section links to "Public sector salary disclosure background and FAQ". Below the main text, an "On this page" section lists two items: "1. Public sector salary disclosure for 1996 to 2017" and "2. Guide and forms for 2018 (disclosure for 2017)". At the bottom, a paragraph of text describes the Public Sector Salary Disclosure Act, 1996, which requires organizations receiving public funding to disclose employee salaries and benefits.

The screenshot shows the Ontario government website's interface for "Travel, meal and hospitality expenses". The header includes the Ontario logo, a search bar, and a "Topics +" menu. The main heading is "Travel, meal and hospitality expenses". Below it, a paragraph explains that users can browse or search work-related expenses claimed by government employees, elected officials, and political staff. It also mentions a "Show/hide columns" button and sorting options. A "View expenses by fiscal year" dropdown menu is set to "2014-2015". Below this, a "Search" section includes a search bar, dropdown menus for "All staff" and "All months", and a "Show/hide columns" button. A table of checkboxes allows users to customize the columns displayed in the results, including Name, Purpose, Title, Start Date, Type, End Date, Destination, Attendees, Other Attendees, Air Fare, Other Transportation, Accommodation, Meals, Incidentals, Subtotal, Hospitality, Other Expenses, and Total.

# Emergency and Compassionate Situations

Personal information can be released in situations where it is necessary to protect the health or safety of an individual, or in compassionate circumstances, where disclosure is necessary to facilitate contact with loved ones



Yes, you can share information with a Children's Aid Society to protect a child.

**YES,**

**YOU**

**CAN.**

**DISPELLING THE MYTHS ABOUT  
SHARING INFORMATION WITH  
CHILDREN'S AID SOCIETIES.**

Find out more at [www.ipc.on.ca](http://www.ipc.on.ca)

# 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

Cont'd

- 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;



# 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*



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.

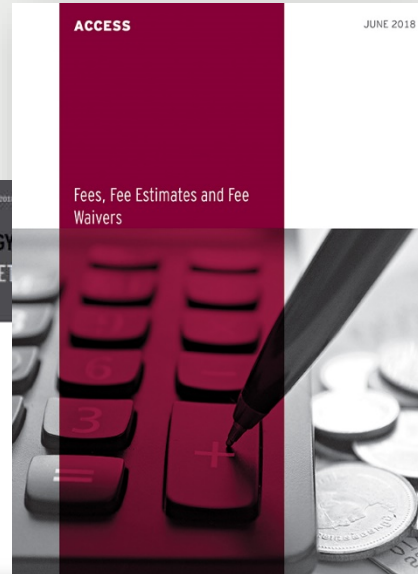
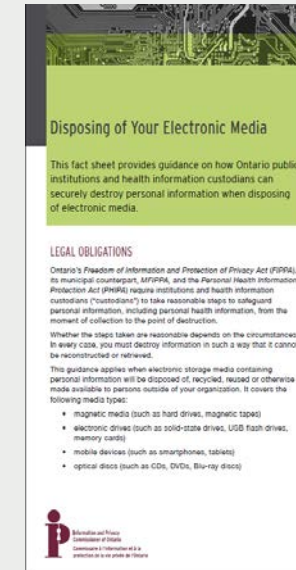
Generally, institutions should disclose personal information to a law enforcement agency *only when required by law*, such as in response to a court order, rather than a simple request, where there is no requirement to disclose.

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.

# IPC Fact Sheets

- Published in response to frequently asked questions about access, privacy and technology
- Recently released:
  - Fees, Fee Estimates and Fee Waivers
  - Frivolous and Vexatious Requests
  - Disposing of Your Electronic Media



## REACHING OUT TO ONTARIO

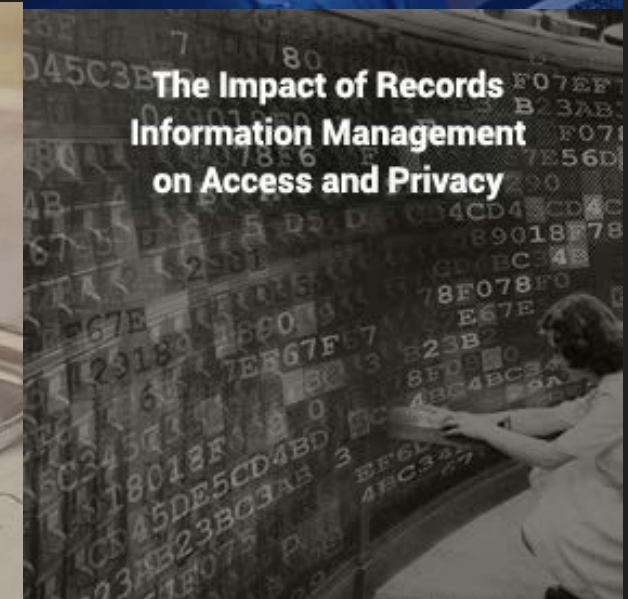
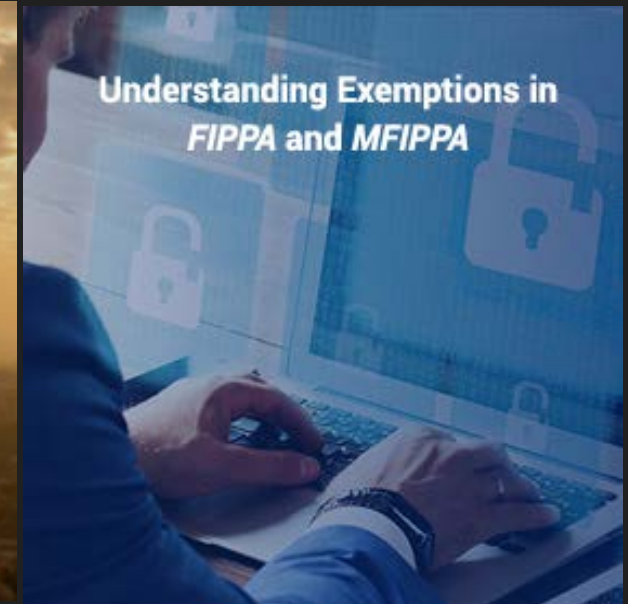
ROTO is an ongoing program where we visit communities across Ontario and host events to discuss the latest developments in access and privacy with stakeholders and the public



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

# 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](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