REACHING OUT TO ONTARIO

Latest Developments at the IPC

Brian Beamish

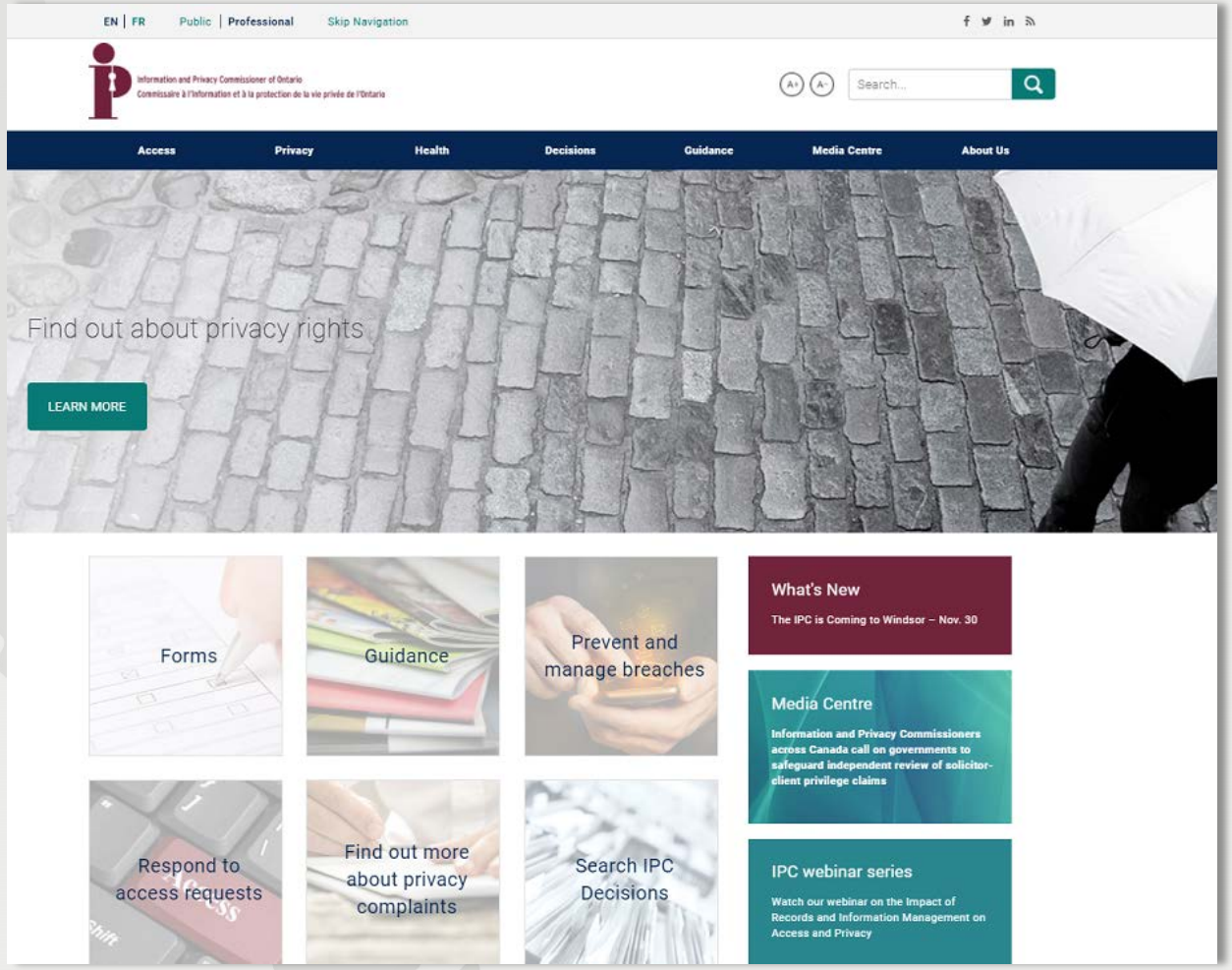
Information and Privacy Commissioner of Ontario

HAMILTON

May 11, 2018

Our Office

- Commissioner appointed by, and reports to, the Legislative Assembly to ensure impartiality
- Provides independent review of government decisions and practices on access and privacy
- Oversees compliance with three access and privacy laws

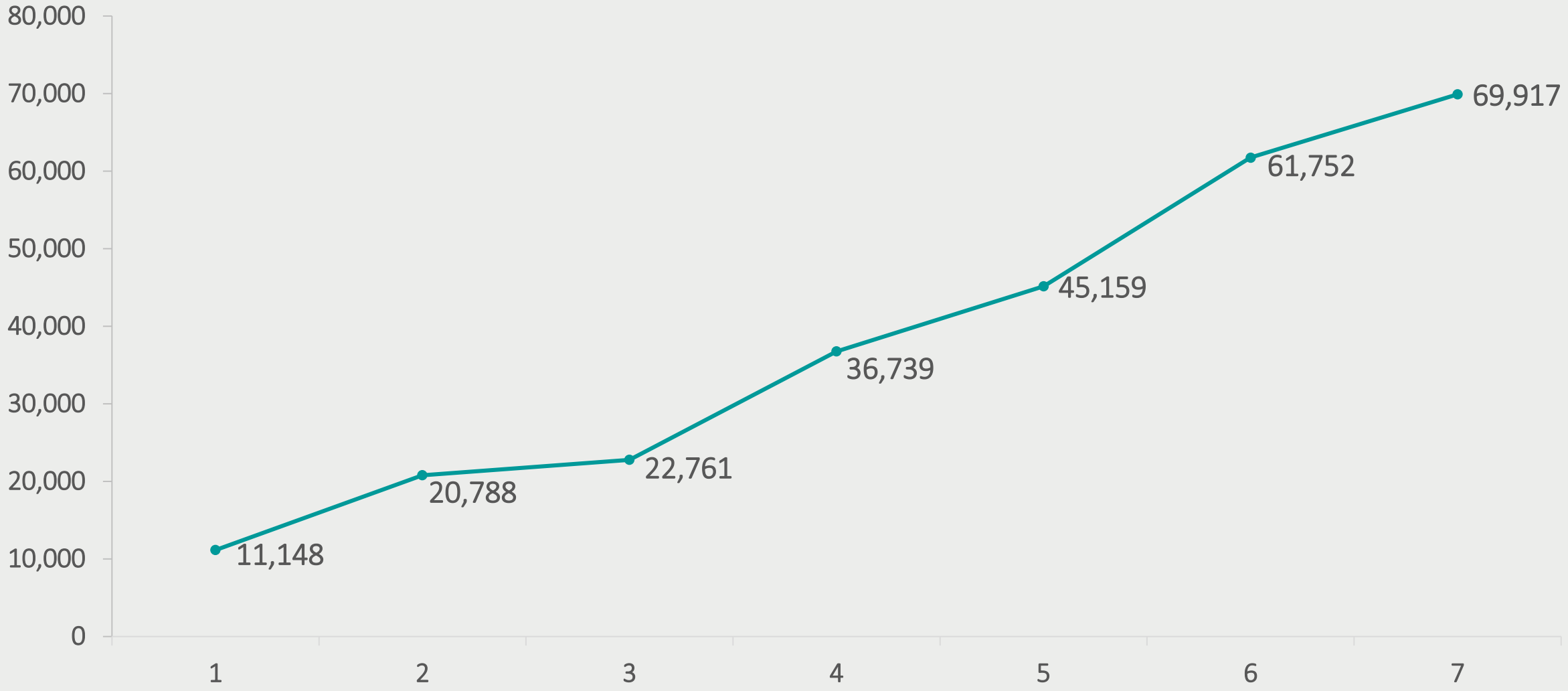


IPC's Mandate

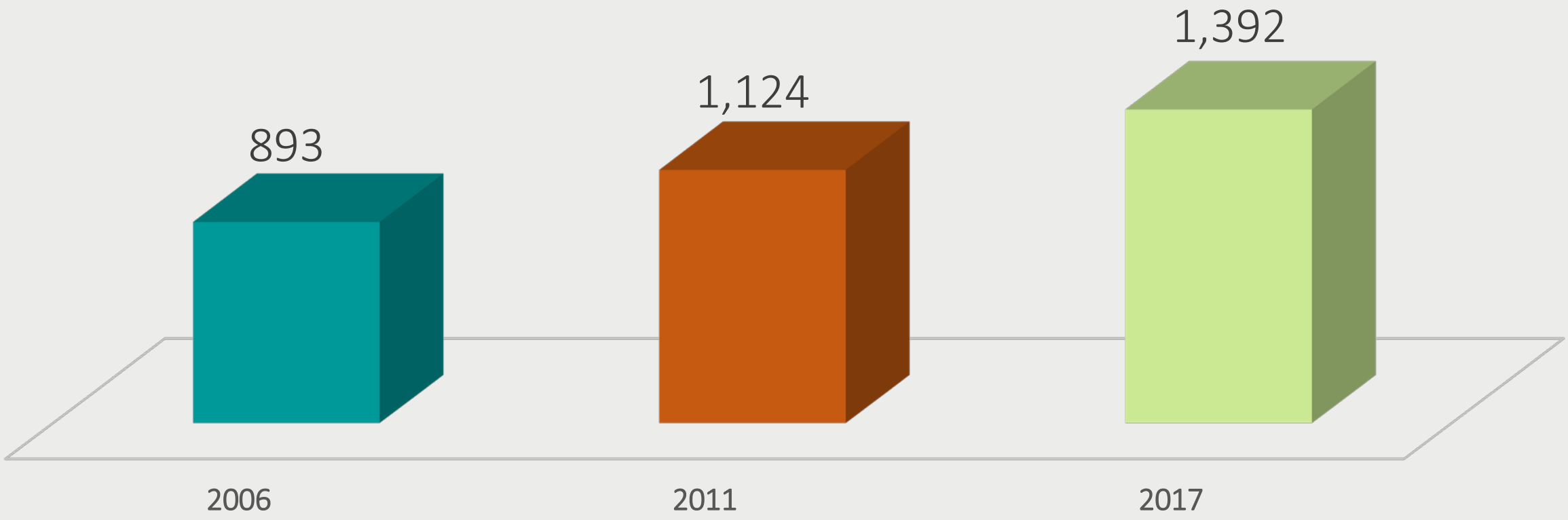
- *Freedom of Information and Protection of Privacy Act* (*FIPPA*)
  - Covers 300 provincial institutions
- *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)
  - Covers 1,200 municipal organizations
- *Personal Health Information Protection Act* (*PHIPA*)
  - Covers individuals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

ACCESS

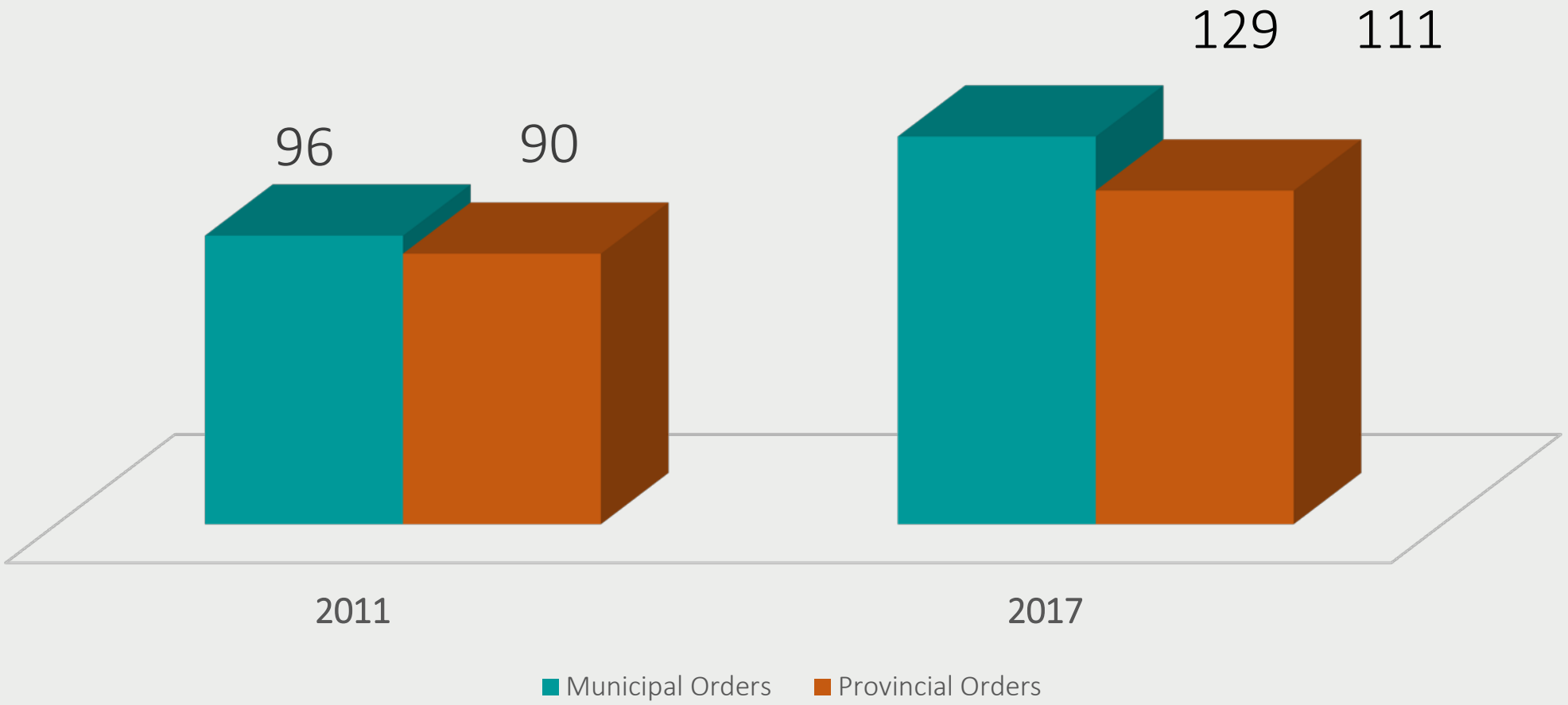
Access Requests per Year



Appeals Received per Year



Access to Information Orders



Mediation: Critical to Our Success

- Usually, 75 per cent of appeals and almost all privacy complaints are closed before adjudication/investigation
- Goal is to find a resolution which satisfies the needs of all involved
- Saves significant time and resources for all parties

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

Smart Cities

- Benefits
  - improved management of urban environments
  - more effective and efficient service delivery
  - innovation and economic development
- Personal information collected, used, retained and disclosed can include:
  - energy consumption patterns
  - video and audio recordings
  - vehicle licence plate numbers
  - mobile device and other identifiers

Privacy Risks of Smart Cities

- Information may be collected by municipalities, contractors, or private sector companies
  - unauthorized collection of personal information and surveillance
  - personal information used for unauthorized secondary purposes
  - unauthorized disclosures of personal information
- Must ensure smart cities do not become infrastructures for mass surveillance

Minimize Privacy Risks

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

Fact Sheet

- Developed to help the public understand smart cities and the impact they can have on personal privacy

APRIL 2018

TECHNOLOGY FACT SHEET

Smart Cities and Your Privacy Rights

New technologies promise to help municipalities better manage urban environments and deliver services in a more effective and efficient way. They can help to make communities more liveable, sustainable, and fair. Many involve the collection and use of large amounts of information, including personal information. Cities or municipalities that use these connected technologies are often described as "smart cities."

This fact sheet was developed to help members of the public understand smart cities and how they can impact an individual's privacy

The Office of the Information and Privacy Commissioner of Ontario (IPC) provides independent oversight of the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*). This act protects the privacy of personal information by setting rules for its collection, use and disclosure by municipalities and municipal institutions. These rules also give individuals the right to access their own personal information.

The IPC has developed this fact sheet to help the public understand smart cities and how they can impact an individual's privacy.

WHAT ARE "SMART" CITIES?

Smart cities use technologies that collect data to improve the management and delivery of municipal services, support planning and analysis, and promote innovation within the community. By collecting large amounts of data, often in real-time, municipalities can gain a greater understanding of the quality and effectiveness of their services. For example, commuter traffic flow data can identify congestion

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

Review of Police Oversight Agencies

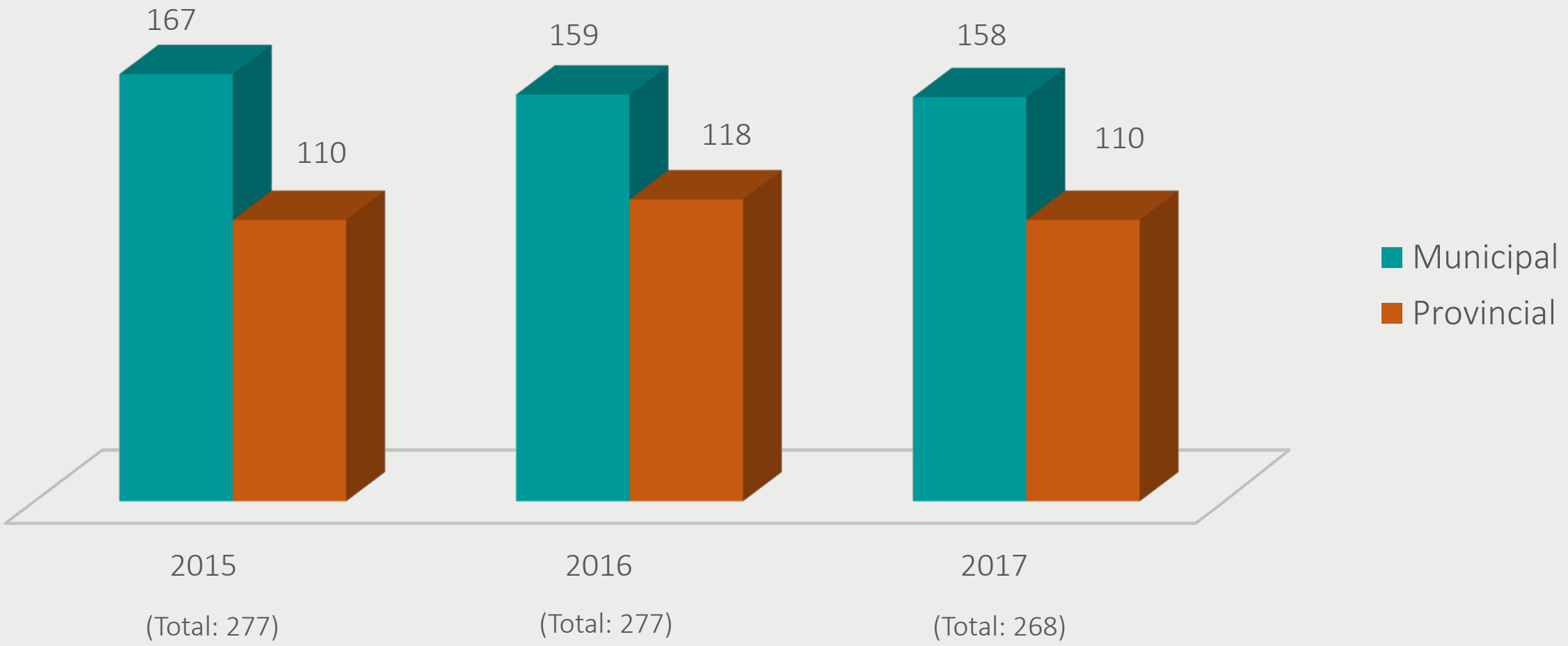
- In 2016, Justice Tulloch appointed to lead independent review of the agencies that oversee police in Ontario
- Three agencies: the Special Investigations Unit, Office of the Independent Police Review Director, Ontario Civilian Police Commission
- IPC provided advice to Justice Tulloch, including:
  - Amending *Police Services Act* to ensure disciplinary hearing decisions, SIU-related disciplinary and investigation reports are made public
  - Establishing police services data collection and retention systems to record human rights-based data on key interactions with civilians

Amendments to the *Police Services Act*

- Change name of Special Investigations Unit to Ontario Special Investigations Unit (OSIU)
- ***Release OSIU reports publicly, include new time limits for the completion and public reporting of investigations***
- Change name of Office of the Independent Police Review Director to the Ontario Policing Complaints Agency (OPCA)
- Authorize OSIU and OPCA to collect personal information specified by regulation and publish reports to inform, evaluate and improve policing oversight

PRIVACY

Public Sector Privacy Complaints 2015 - 2017



The Philadelphia Model

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

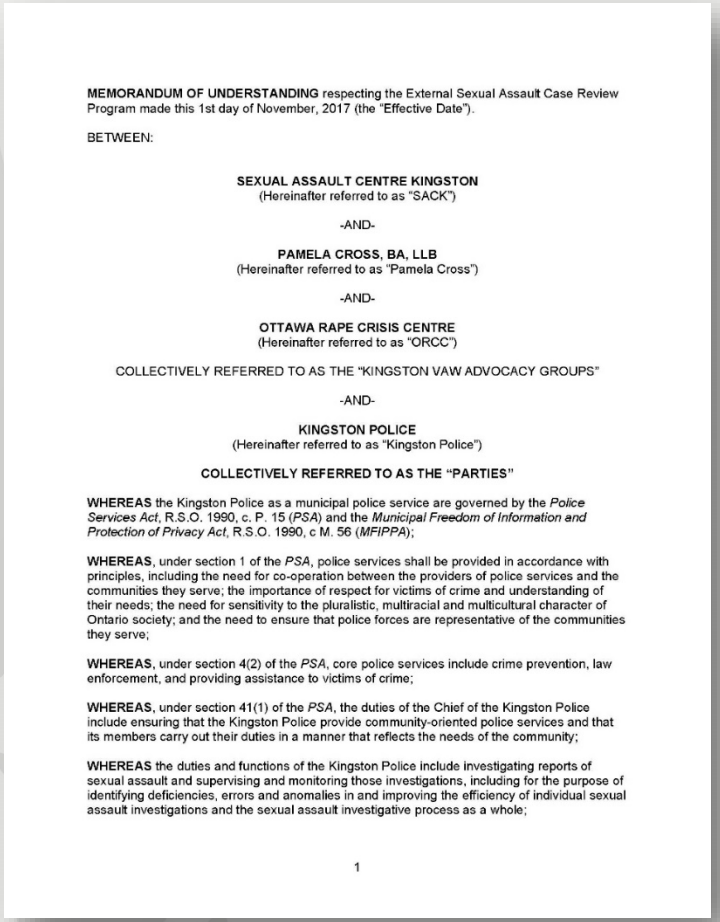
Globe and Mail Series: “Unfounded”

Ontario-based Philadelphia Model

- Identify external partners with the experience to assist with the review of sexual assault files and appoint them agents of the service
- Ensure external reviewers have background check, sign an oath of confidentiality and receive privacy and confidentiality training
- Require external reviewers to see names of principals so they can recuse themselves if needed
- Permit external reviewers to review complete closed files, subject only to redactions or restrictions required by law
- Ensure reviews take place at police facilities and no identifying information is copied, retained, or removed by agents

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;

1

Public Health Release of Flu Death Information

- Hamilton public health refused to disclose the number of flu deaths in the community to a reporter from the Hamilton Spectator, citing privacy of personal health information
- The reporter contacted the IPC for guidance and whether the public's right to know outweighs privacy considerations
- The reporter pointed to another community that issued a public alert when two patients died of the flu in the same week and made public what strain of the flu they had
- The IPC encourages public institutions to be as transparent as possible and release non-identifiable information that would be of interest to the public

Video Surveillance

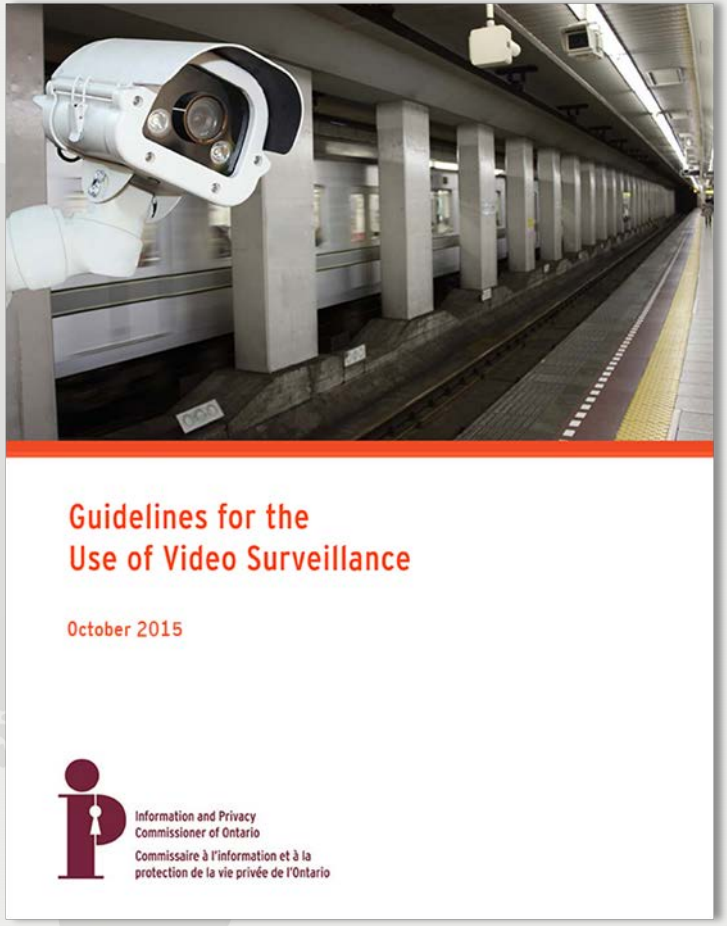
- Surveillance technologies can enhance public safety but must protect privacy and respect privacy laws
- Privacy implications:
  - potential to collect large amounts of personal information about individuals
  - ability to track locations of individuals over time
  - profiles law-abiding individuals going about everyday activities

Video Surveillance in Hamilton

- 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
- Privacy implications of change include:
  - invasive surveillance of neighbours
  - ability to track the locations of individuals over time and enable profiling
- Public institutions are required to protect personal information, and to follow strict rules when collecting, using and disclosing
- Hamilton is encouraged to leave the by-law unamended

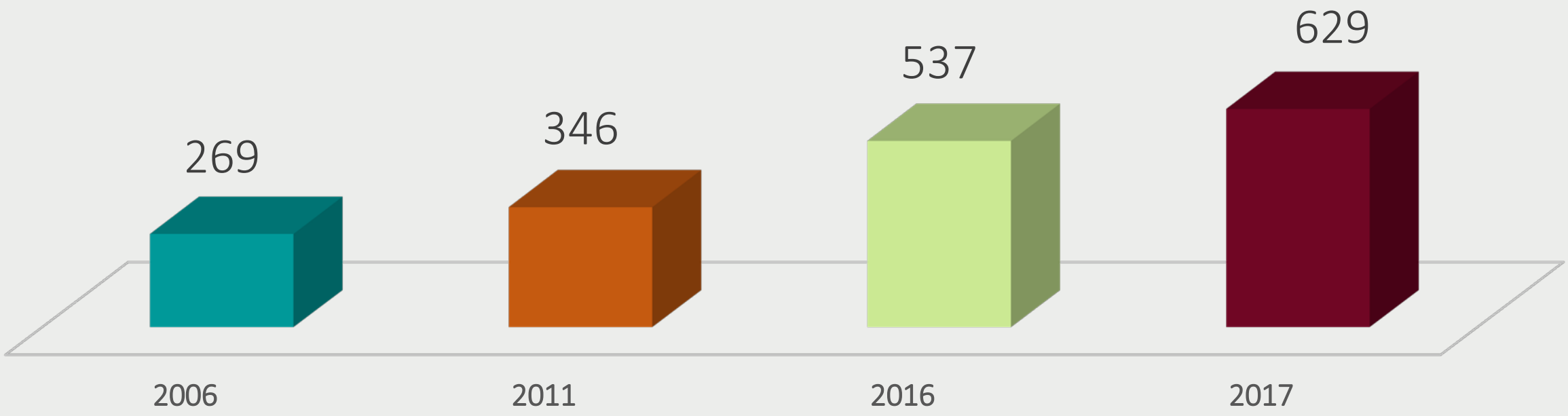
Video Surveillance Guidelines

- Updated guide consolidates previous advice and presents new factors to consider, including retention periods and notices of collection



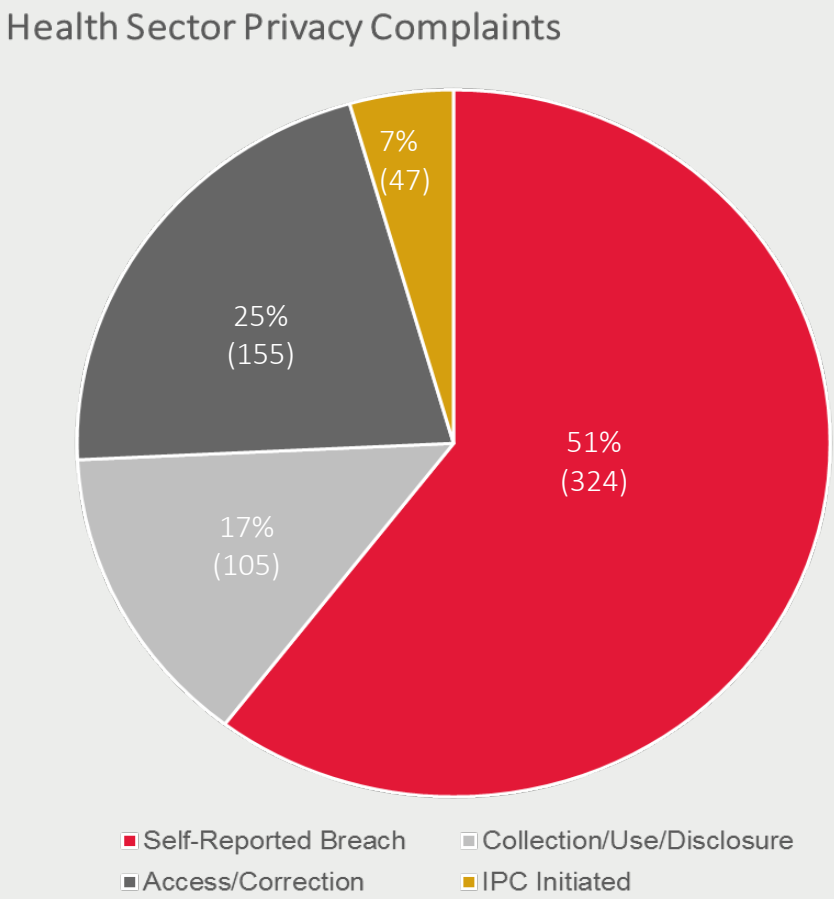
HEALTH PRIVACY

PHIPA Complaints Opened per Year



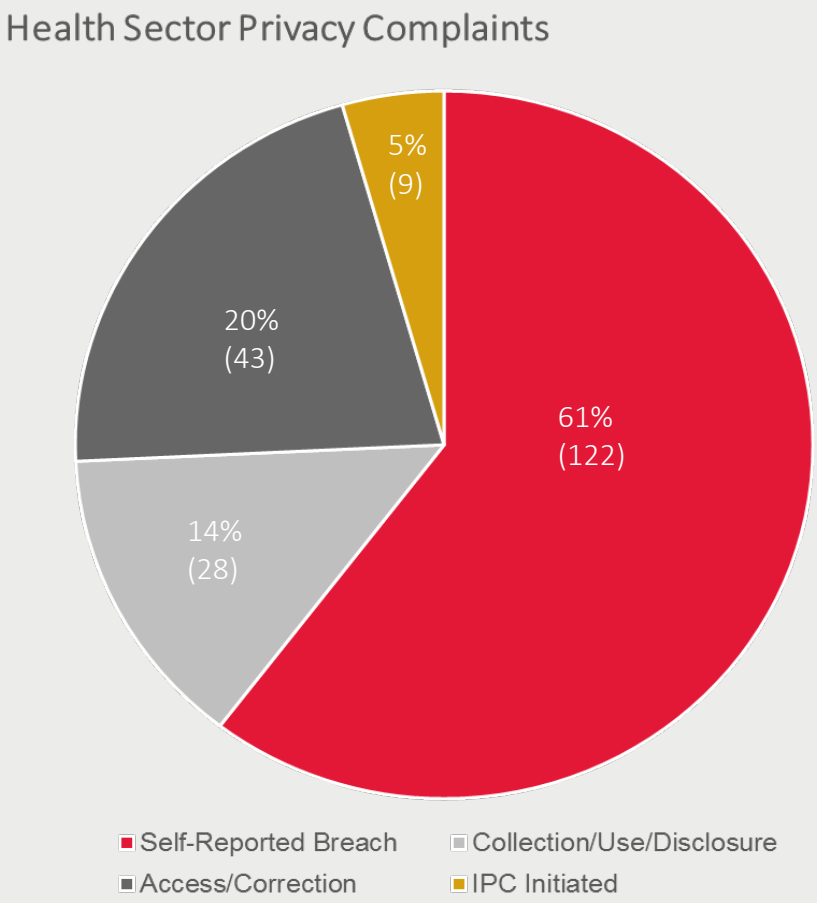
Health Sector Privacy Complaints 2017

- Of the 324 self-reported breaches in 2017:
  - 60 were snooping incidents
  - 8 were ransomware/cyberattack
- Remaining 256 were related to:
  - lost or stolen PHI
  - misdirected information
  - records not properly secured
  - other collection, use and disclosure issues



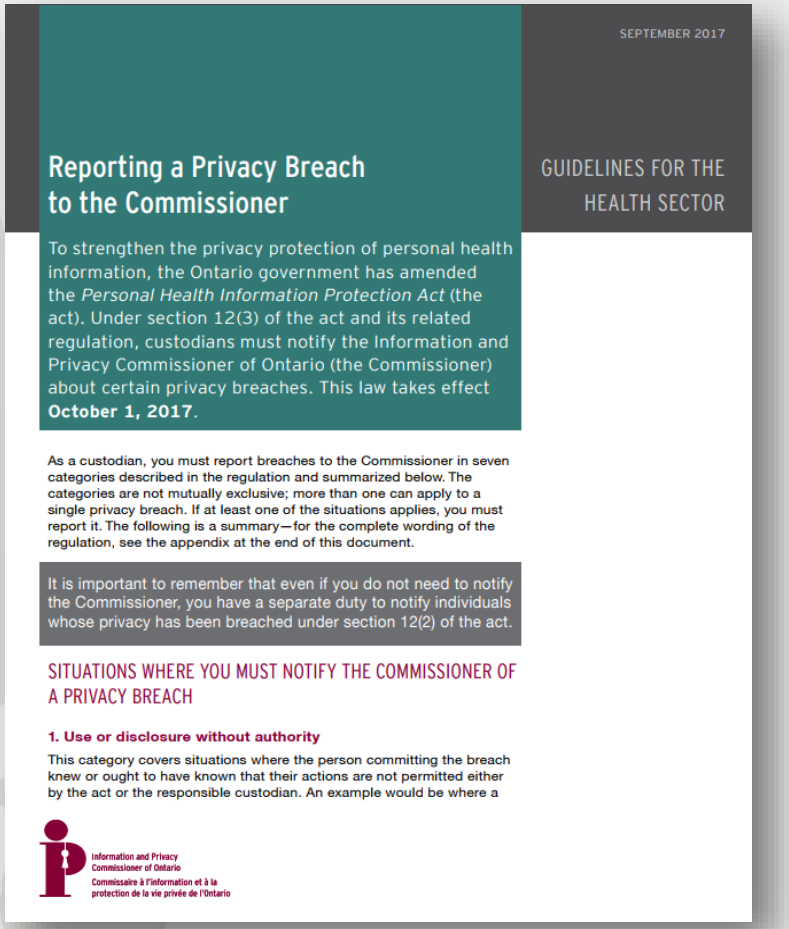
Health Sector Privacy Complaints 2018

- Of the 122 self-reported breaches in 2017:
  - 23 were snooping incidents
  - 2 were ransomware/cyberattack
- Remaining 97 were related to:
  - lost or stolen PHI
  - misdirected information
  - records not properly secured
  - other collection, use and disclosure issues



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



SEPTEMBER 2017

Reporting a Privacy Breach to the Commissioner

GUIDELINES FOR THE HEALTH SECTOR

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.

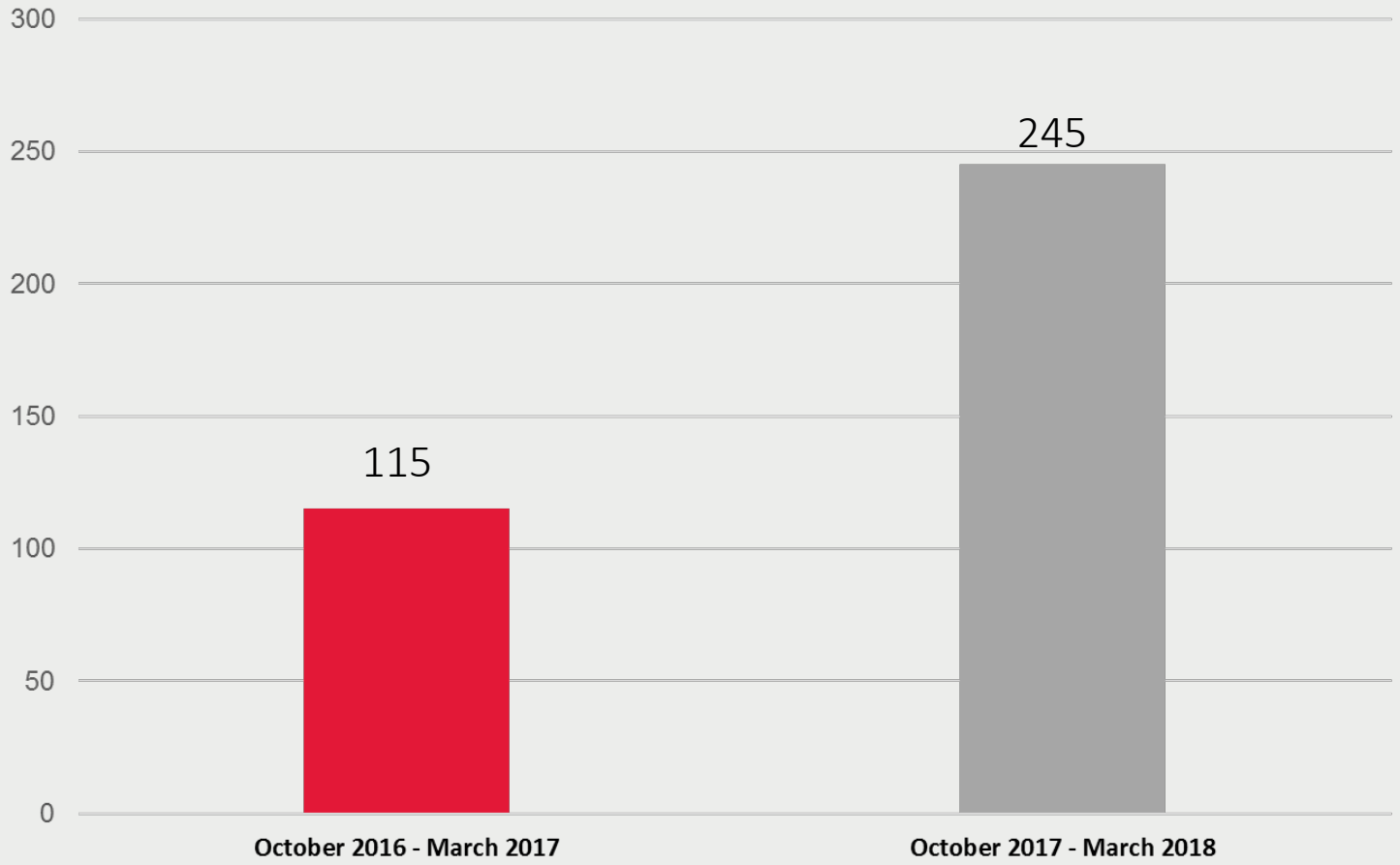
SITUATIONS WHERE YOU MUST NOTIFY THE COMMISSIONER OF A PRIVACY BREACH

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

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

Self-Reported Breaches
Before and After Mandatory Breach Reporting



Recent PHIPA Prosecution

- 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, 2108, 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 protects privacy by creating rules regarding personal information:
  - collection
  - use
  - disclosure
  - retention
  - disposal
- Data minimization requirements limit a service provider's authority to collect, use or disclose personal information

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)

Child, Youth and Family Services Act

- Under new law, when responding to access requests, service providers must:
  - make the record available or provide a copy, if requested
  - respond to the request within 30 days, with a possible 90-day extension
  - take reasonable steps to be satisfied of the individual's identity

Anti-Racism Act

- In June 2017, Ontario passed the *Anti-Racism Act, 2017* (ARA)
- Under this legislation, the government is responsible for developing and maintaining an anti-racism strategy that aims to eliminate systemic racism and advance racial equality
- The government is required to consult with the IPC on the development of the data standards to ensure robust privacy protections are in place
- In addition, the IPC is the oversight body for the ARA
- We can receive and investigate privacy complaints and order an organization to change or discontinue how it handles personal information if a practice contravenes the ARA or the standards

Next – Panel Sessions

Session A: Key Developments in Access and Privacy (Lower Auditorium)

- Brian Beamish, Commissioner
- David Goodis, Assistant Commissioner

Session B: Protecting Personal Health Information (Upper Auditorium)

- Suzanne Brocklehurst, IPC Registrar
- Debra Grant, Director of Health Policy

CONTACT US

Office of the 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