

Access and Privacy in Ontario: Latest Developments

Brian Beamish

Information and Privacy Commissioner
of Ontario



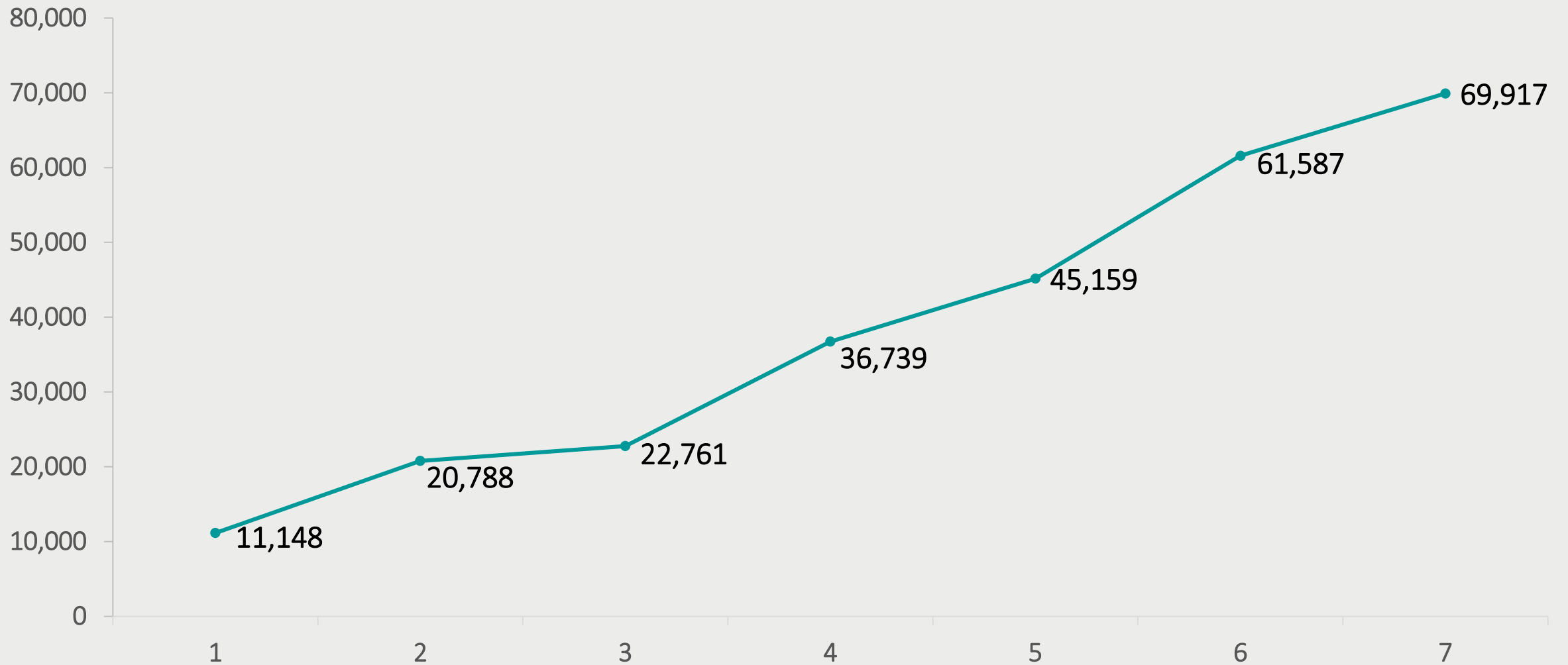
Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

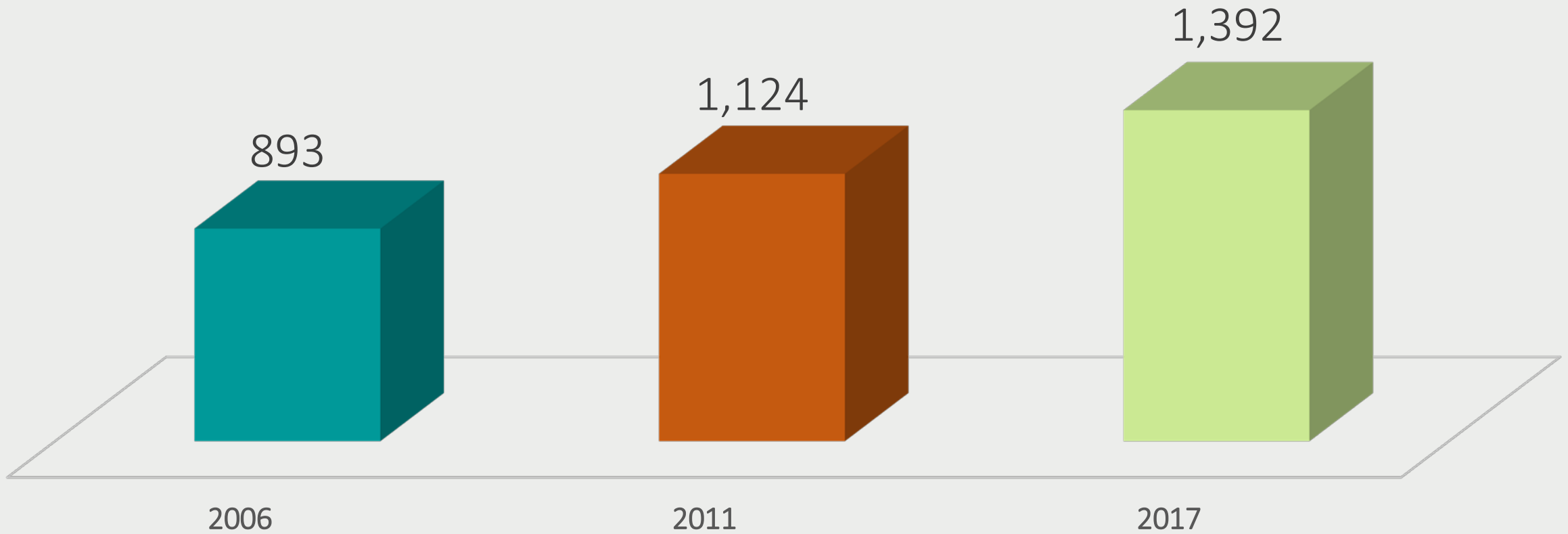
Ontario
Connections

May 31, 2018

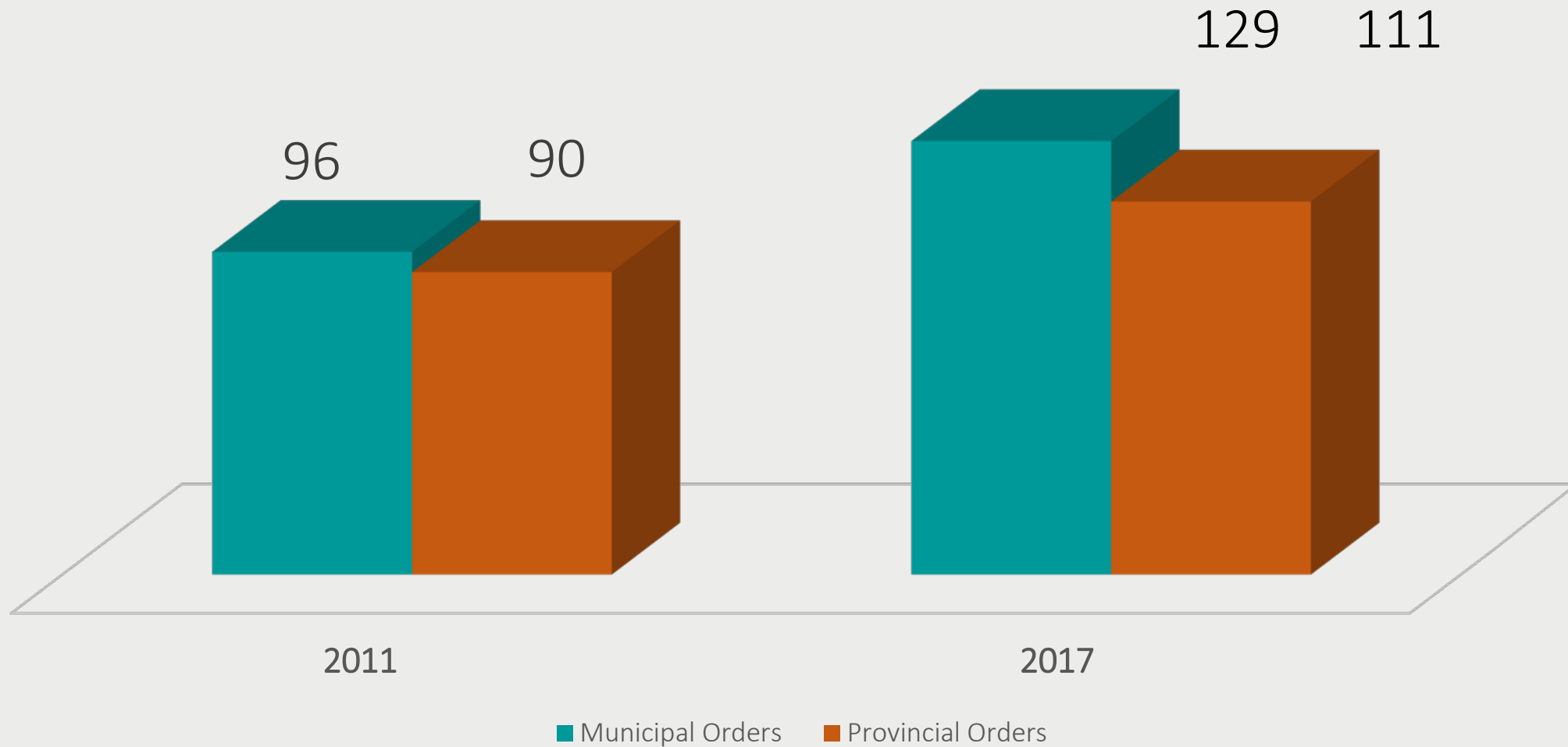
Access Requests per Year



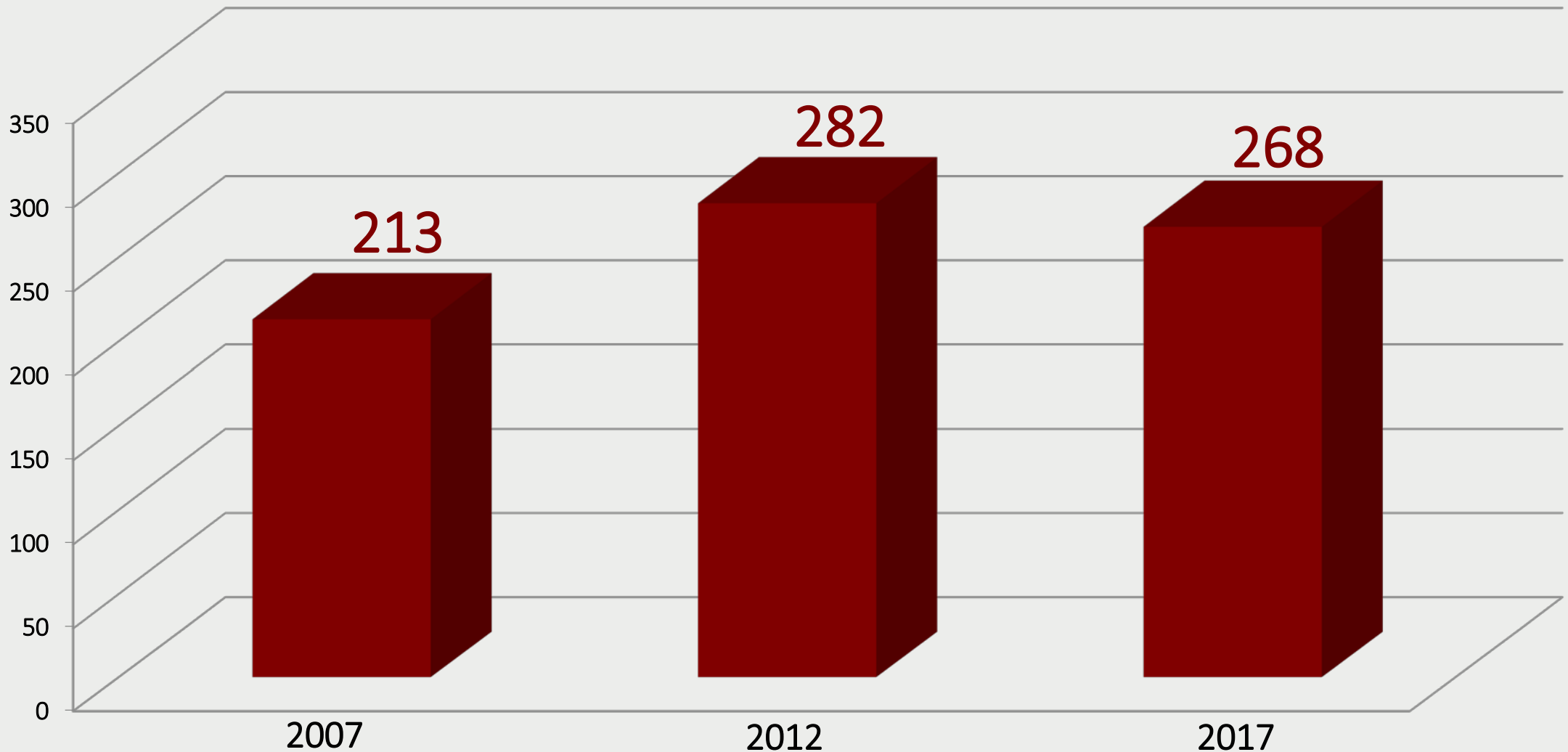
Appeals Received per Year



Access to Information Orders



Total Privacy Complaints Opened Per Year



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

- Communities that use connected technologies 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

Cont'd

- 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

Cont'd

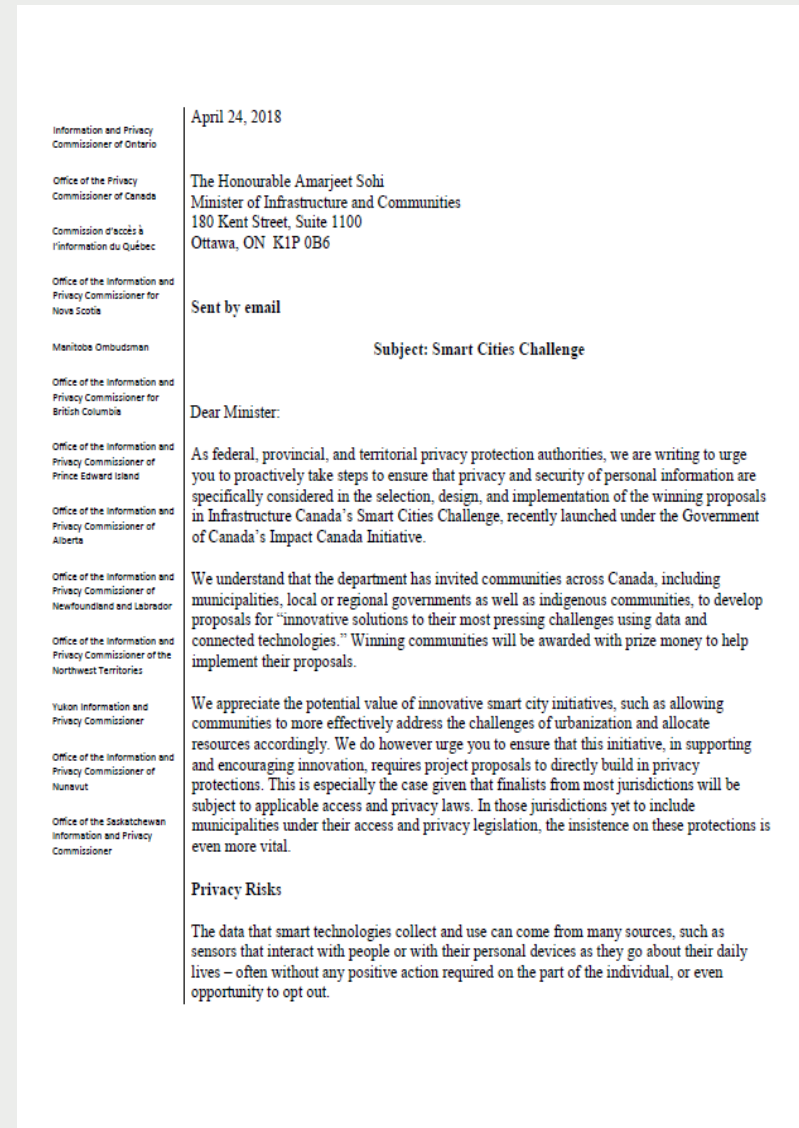
- Information may be collected by municipalities, contractors, or private sector companies
 - unauthorized collection of personal information and surveillance
 - personal information used for unauthorized secondary purposes
 - unauthorized disclosures of personal information
- Must ensure smart cities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



Smart Cities: Minimize Privacy Risks

Cont'd

- 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



Smart Cities Fact Sheet

- Helps the public understand how smart cities can affect privacy
- Information collected, used, retained and disclosed can include personal information
- Great care must be taken to ensure that smart cities do not become infrastructures for mass surveillance
- Good planning and design can minimize risk and ensure that individual privacy is protected



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

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

Ontario-based Philadelphia Model

Cont'd

- 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

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;

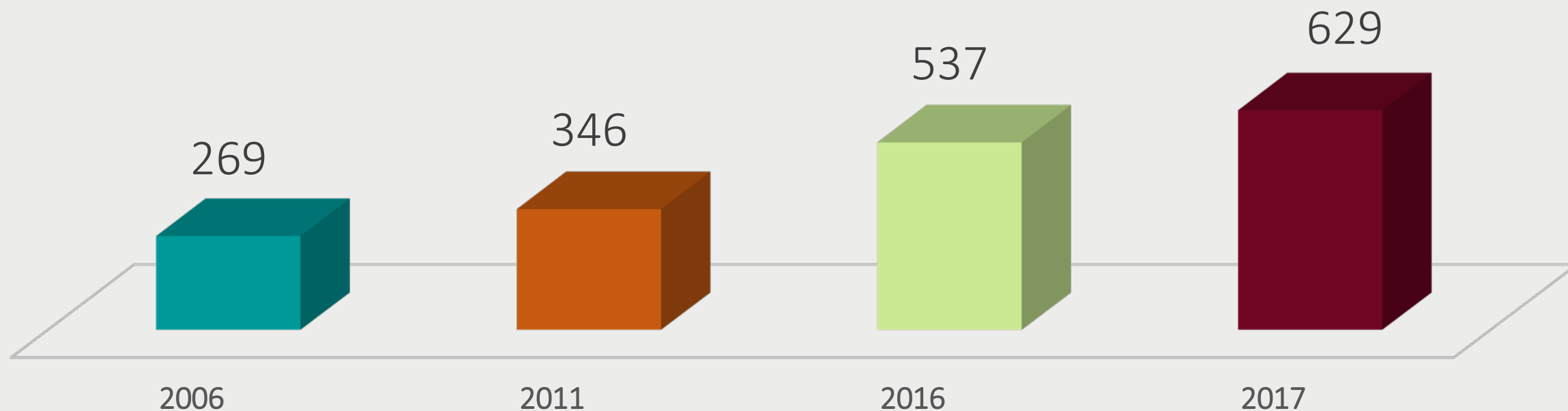
Making Political Parties Subject to Privacy Laws

- Political parties are not covered by privacy laws
- Digital tools can amass large amounts of personal information from diverse sources, analyze it and target people in granular and unique ways
- Increasingly sophisticated data practices raise new privacy and ethical concerns and vulnerabilities to cybersecurity threats
- To address these risks, our office recommends that Ontario's political parties be subject to privacy regulation and oversight



Health Privacy

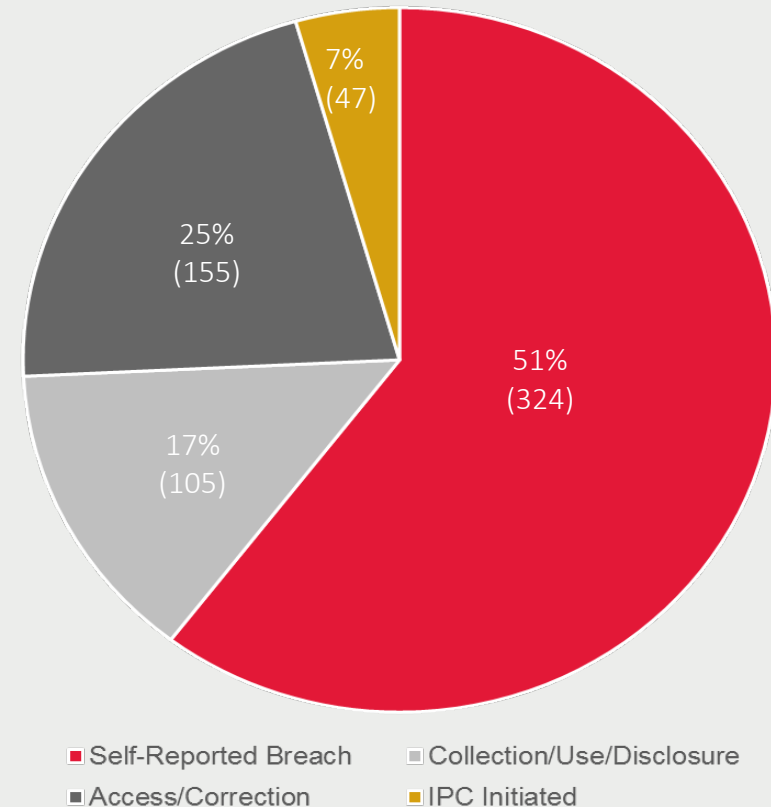
PHIPA Complaints Opened per Year



Health Sector Privacy Complaints 2017

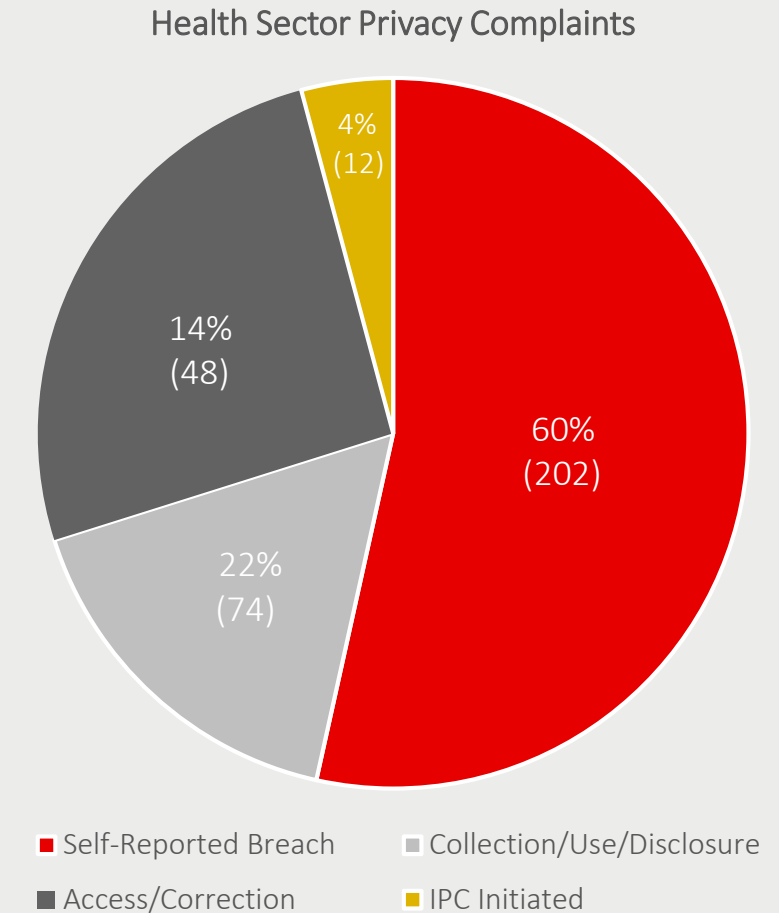
- Of the 324 self-reported breaches in 2017:
 - 60 were snooping incidents
 - 8 were ransomware/cyberattack
- Remaining 256 were related to:
 - lost or stolen PHI
 - misdirected information
 - records not properly secured
 - other collection, use and disclosure issues

Health Sector Privacy Complaints



Health Sector Privacy Complaints 2018

- Of the 202 self-reported breaches in 2018:
 - 44 were snooping incidents
 - 4 were ransomware/cyberattack
- Remaining 154 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

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.

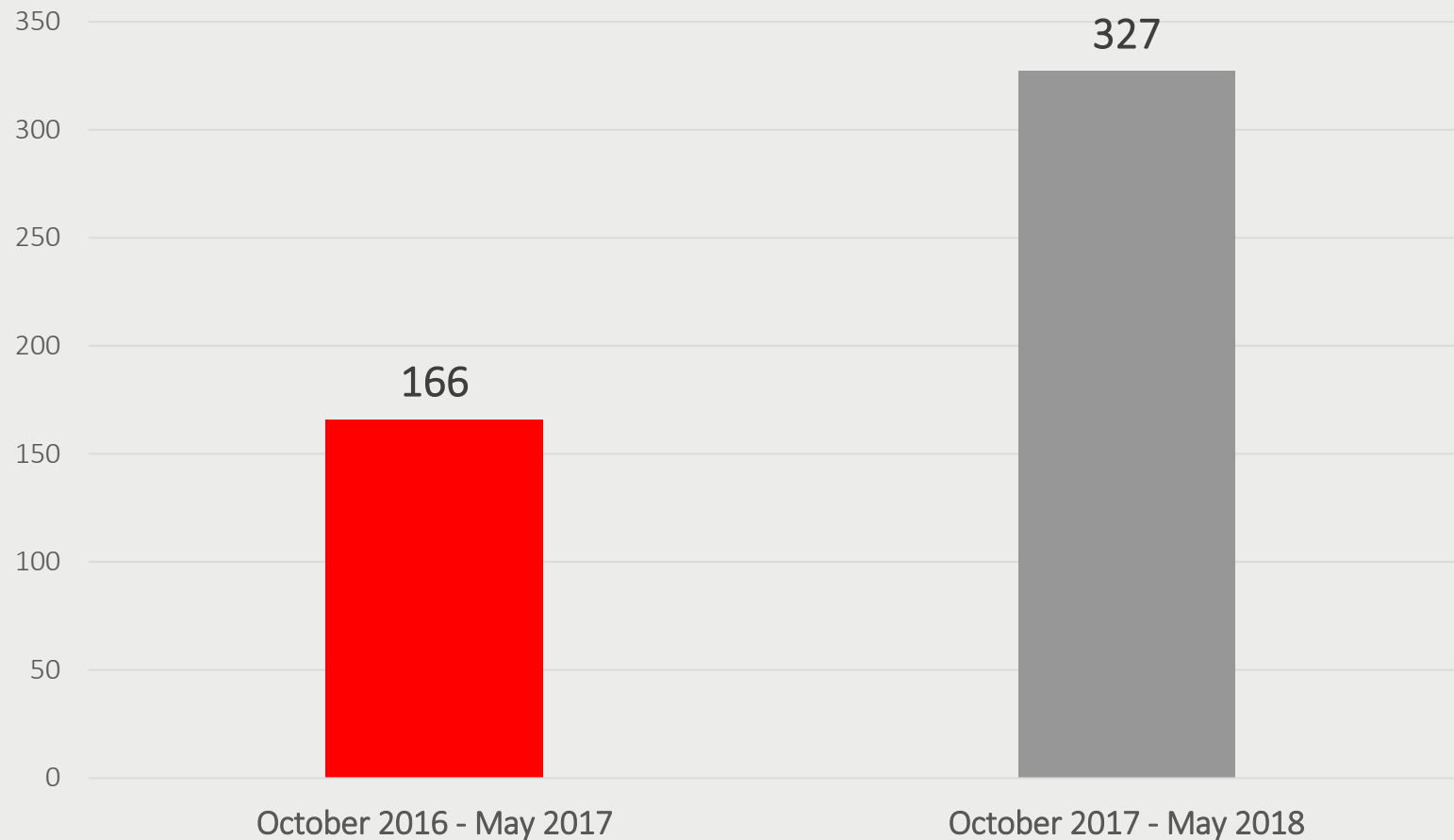
It is important to remember that even if you do not need to notify the Commissioner, you have a separate duty to notify individuals whose privacy has been breached under section 12(2) of the act.

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



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

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

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 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)
- The government launched the ARA's data standards and approved Regulation 267 in April 2018
- Regulation requires PSOs in child welfare, education and justice sectors to start collecting Indigenous identity, race, religion and ethnic origin by a defined date in the next five years
- The government consulted the IPC on the data standards
- IPC is the oversight body and may:
 - order public sector organizations (PSOs) to discontinue, change or implement a practice, and destroy personal information collected
 - comment and make recommendations on privacy implications of any matter related to act, regulations or data standards

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*

Cont'd

- 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

Police Record Checks Reform Act

- Becomes law on November 1, 2018
- Reflects over a decade of input from our office
- Changes the rules about what police can tell prospective employers, volunteer agencies and foreign governments about Ontarians
- Protects individuals from the release of unproven allegations and mental health records in police background checks
- First law of its kind in Canada

TORONTO STAR

News · Investigations

Law protecting Ontarians from disclosure of police records finally gets green light

Nearly three years after it was passed unanimously by the Ontario legislature, the Police Record Checks Reform Act will become law on Nov. 1. It will severely limit the release of police “non-conviction records” that have thwarted careers and ruined lives, as detailed in a Star investigation.



By **ROBERT CRIBB** Investigative Reporter
Mon., May 7, 2018





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.

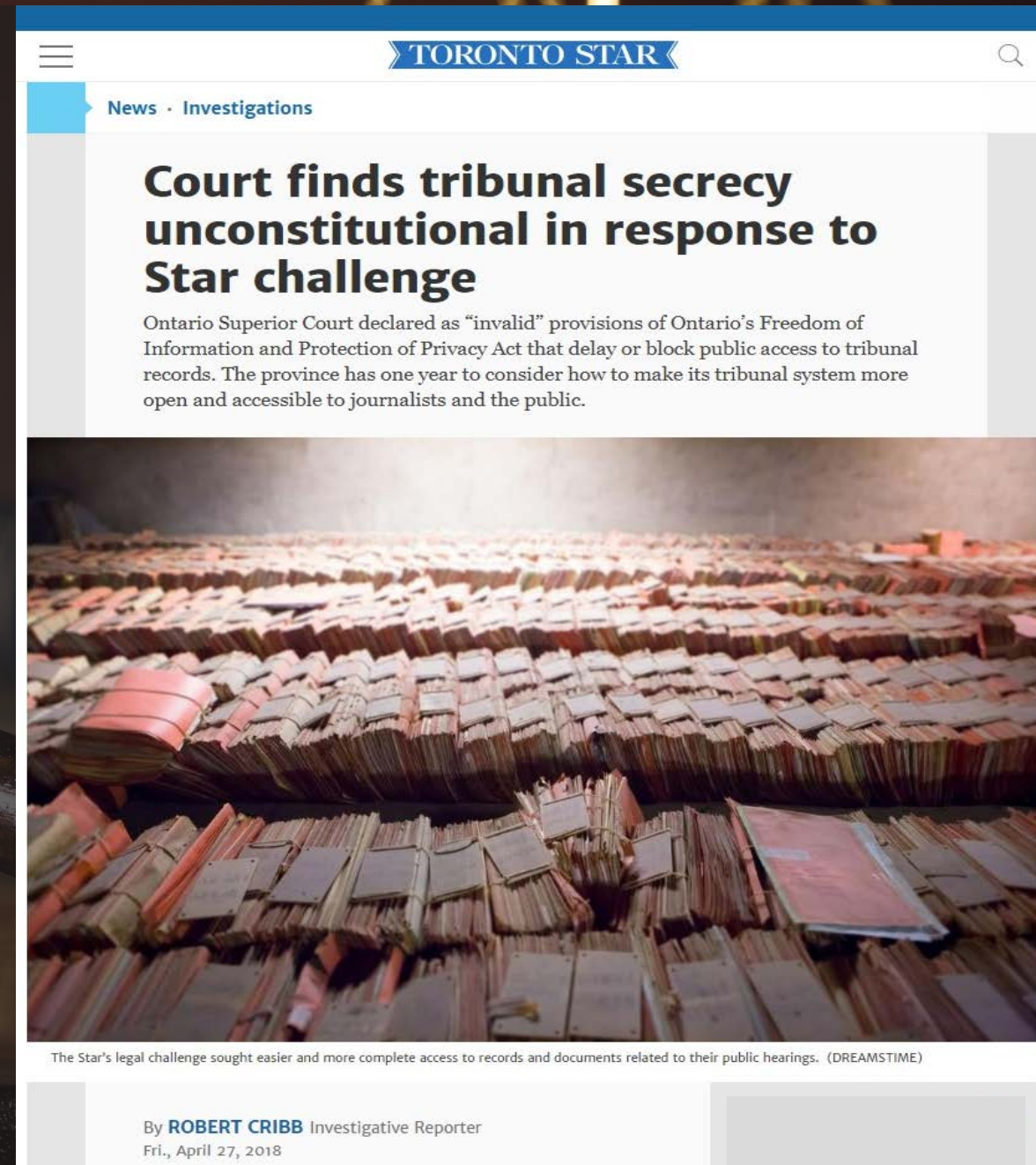


Reasonable Expectation of Privacy: *Jarvis* (SCC)

- 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

“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 header includes the Toronto Star logo and a search icon. The article is categorized under 'News · Investigations'. The main headline reads '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 photograph of numerous stacks of papers, some bound with red rubber bands, suggesting a large volume of records. 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)'

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

Resources

IPC Guidance Documents

- Police services are using ALPR systems to find licence plates that are stolen, expired or registered to suspended drivers
- These systems have the potential to track individuals allowing police to conduct surveillance and profiling
- We encourage police services to consult with our office before implementing an ALPR system
- We can help mitigate privacy issues that may arise

Guidance on the Use of Automated Licence Plate Recognition Systems by Police Services

IPC Fact Sheets

- Published in response to frequently asked questions about access, privacy and technology
- Recently released:
 - Fees, Fee Estimates and Fee Waivers (Friday?)
 - 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
- London
- Thunder Bay
- Windsor
- Hamilton

IPC Webinar

The Impact of Records and Information Manage...  

**The Impact of Records and Information Management
on Access and Privacy**



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

0:06 / 12:51

  **YouTube** 

The video player shows a woman in a white lab coat looking at a large wall of data. The wall is covered in a grid of small, glowing icons, each with a unique alphanumeric code. The overall aesthetic is futuristic and data-driven.

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