

# Key Updates from 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

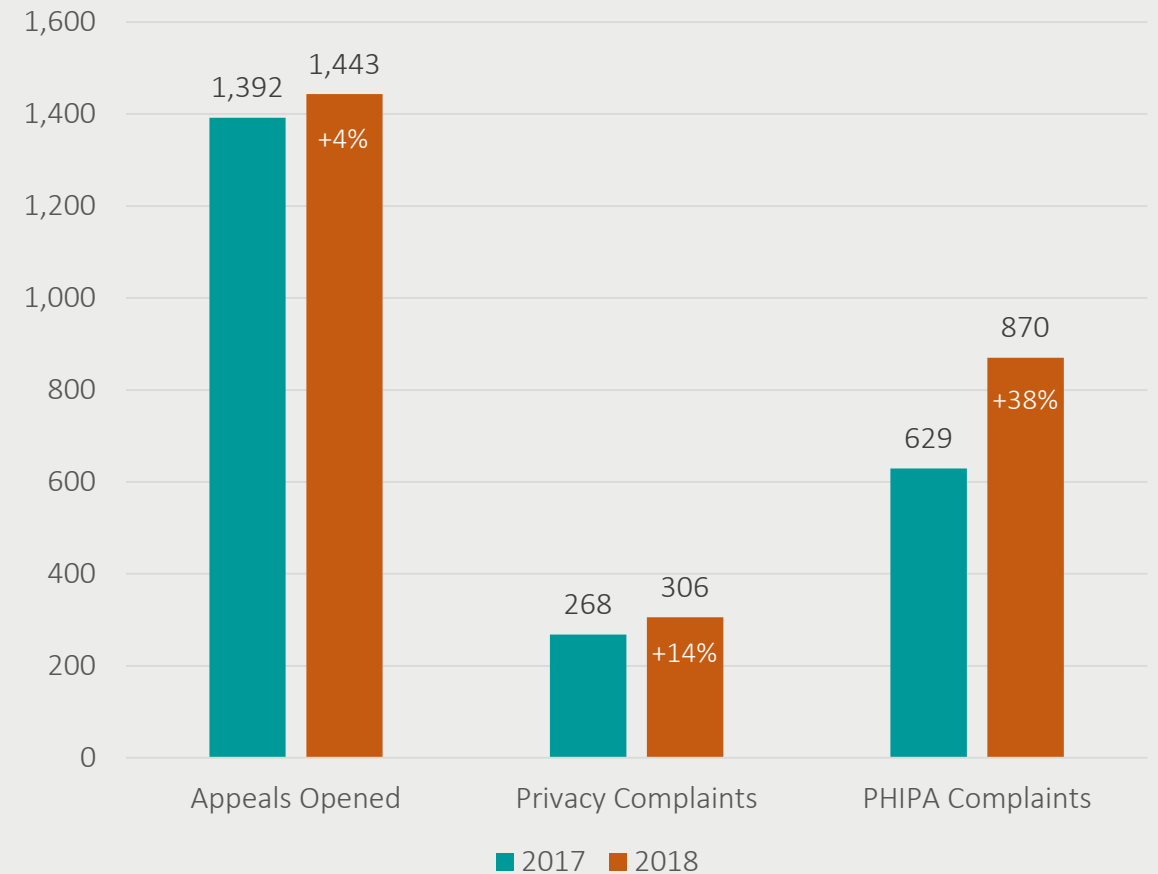
Ontario Bar Association  
Toronto, Canada

April 3, 2019

# 2018: Busy Year

- 1,443 Appeals opened
- 306 Privacy complaints received
- 870 *PHIPA* (health privacy) complaints

Getting Busier: 2017 vs. 2018



# Data Integration

- Sharing, linking, analyzing data across agencies can result in new insights for:
  - policy development
  - system planning
  - resource allocation
  - performance monitoring
- *FIPPA/MFIPPA* does not permit disclosure for these purposes

# Privacy Risks of Data Integration

- Not based on consent – lack of transparency
- Creation of multiple massive government databases of personal information
- Surveillance and profiling of individuals
- Increased cybersecurity risks
- Potential discrimination based on inaccurate data/flawed algorithms

# IPC and Ontario Government Working Group

- IPC and Ontario Government staff are working to design a legislative framework to enable a centralized approach to data integration
- Benefits of a centralized approach:
  - no duplication of linked datasets across multiple government agencies
  - consistent application of privacy controls
  - independent oversight
  - public trust and accountability

# IPC's Proposed Legislative Framework

- Enable **inter-ministerial data integration**
- Require a single dedicated unit within the OPS to:
  - collect and link personal information on behalf of ministries
  - de-identify information
  - make only de-identified information available to ministries for system planning, analysis and evaluation
- Establish framework for privacy controls – section 55.9 of *PHIPA* model
- Enhance investigative/audit/order making powers of the IPC

# 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

- 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 and disclosing information for other purposes without consent (**function creep**)
  - security breaches (**cyberattacks**)

# Which Privacy Laws Apply?

## *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*

- No **collection** of personal information unless:
  - authorized by statute
  - used for law enforcement
  - when necessary for a lawfully authorized activity
- No **use** or disclosure unless for the same, or a consistent, purpose

## *Personal Information Protection and Electronic Documents Act (PIPEDA)*

- Data collected by **private sector** for commercial purpose
  - organization must get meaningful consent
  - individuals must be given clear information explaining what organization will do with their information

# Our Involvement in Smart Cities

- Public education fact sheet
- Lead on Smart Cities Challenge letter to Infrastructure Canada
  - Reviewed PIA's of Ontario finalists
- Engaged on Quayside
  - Supporting the city and province's review of MIDP



# *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

# Toronto Star v. Ontario Attorney General

- Newspaper seeking easier and fuller access to records of public hearings
- Court agrees *FIPPA* an unreasonable barrier to accessing adjudicative records [*Charter*, s. 2(b)]
  - gives province a year to consider how to make tribunals more open
- Must balance openness with privacy
- Legislation is expected this spring



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

- High school teacher charged with voyeurism
- Used a 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 - students in common areas have objective expectation of privacy, including in areas with existing video cameras
- Supreme Court of Canada ruled the teacher was guilty of voyeurism
- The ruling reinforces the IPC’s position that individuals have an expectation of privacy even though they may be in a public or semi-public space





PHIPA

# 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



# Results of the Pilot

- Initially, many privacy breaches were detected during the six month pilot
- The auditing solution used data analytics and AI to determine what accesses could be explained
- Breaches decreased significantly as the solution was fine tuned and missing information from various information systems (e.g., scheduling) was added
- The number of breaches is expected to decrease further with staff awareness and increased ability for solution to explain accesses

- A CBC Marketplace investigation revealed that a Toronto plastic surgeon, Dr. Six, may have been filming patients in states of undress without their consent
- Surveillance cameras located in consultation rooms
- He is now under investigation by both the College of Physicians and Surgeons of Ontario and our office

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

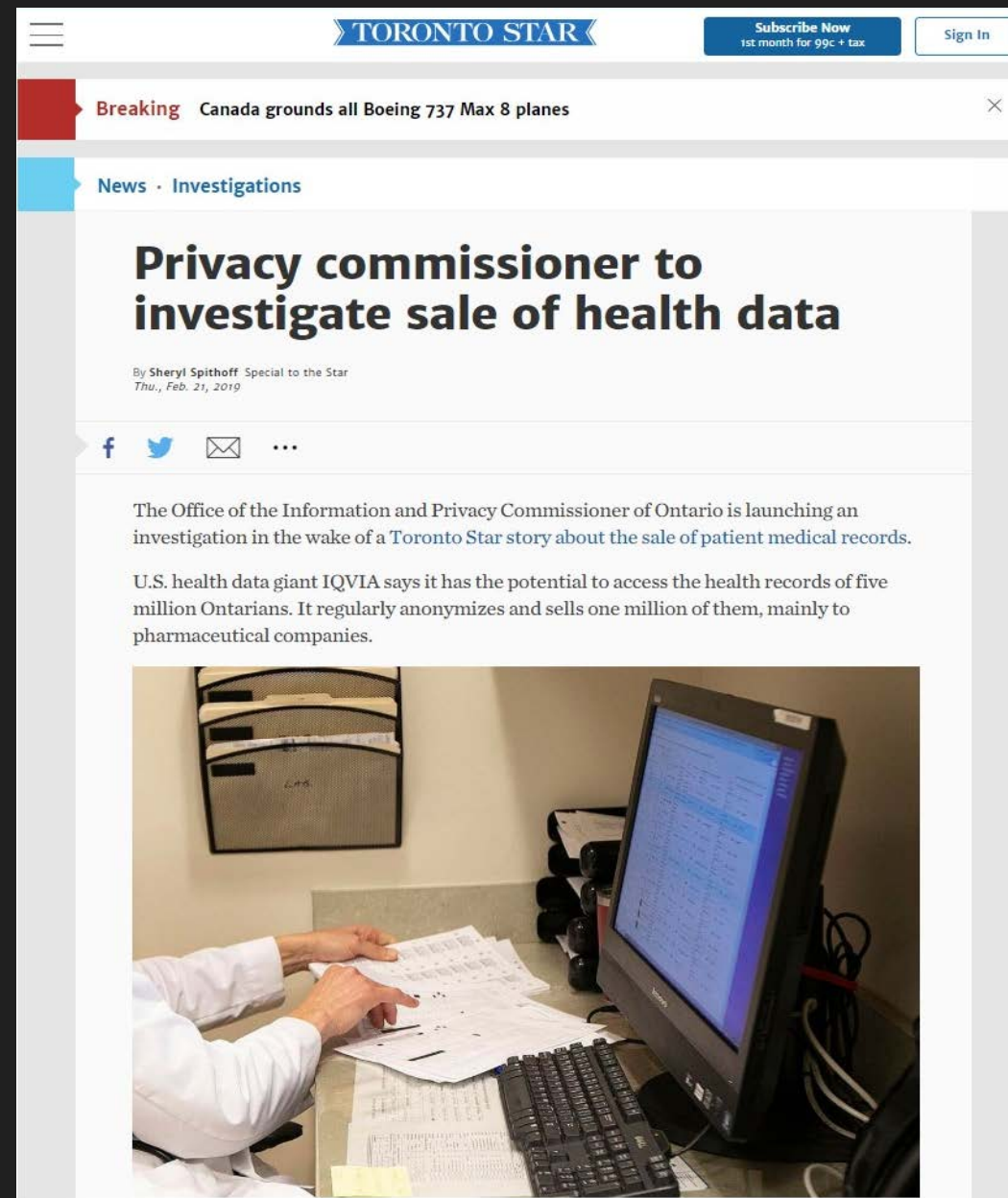
Caitlin Taylor, Makda Ghebreslassie - CBC News ·

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



*“The article indicates that information from patient records is being provided to private sector organizations. We have reason to believe that these arrangements may be contrary to the law.”*

— IPC statement to the Star



The screenshot shows the top of a Toronto Star news page. At the top right, there is a navigation bar with the Toronto Star logo, a 'Subscribe Now' button (1st month for 99c + tax), and a 'Sign In' button. Below this is a red 'Breaking' banner with the text 'Canada grounds all Boeing 737 Max 8 planes'. Underneath is a blue 'News · Investigations' banner. The main headline is 'Privacy commissioner to investigate sale of health data' in large, bold black font. Below the headline, it says 'By Sheryl Spithoff Special to the Star Thu., Feb. 21, 2019'. There are social media sharing icons for Facebook, Twitter, and Email. The article text begins with 'The Office of the Information and Privacy Commissioner of Ontario is launching an investigation in the wake of a Toronto Star story about the sale of patient medical records.' The next paragraph states 'U.S. health data giant IQVIA says it has the potential to access the health records of five million Ontarians. It regularly anonymizes and sells one million of them, mainly to pharmaceutical companies.' Below the text is a photograph of a person in a white lab coat sitting at a desk, looking at a computer monitor and some papers.

The image features a solid teal background. On the left side, there is a large, semi-transparent speech bubble shape in a slightly darker shade of teal. The word "Decisions" is written in white, sans-serif font inside the speech bubble.

Decisions

# Limits to Correction

## *PHIPA Decision 67*

- Complainant submitted a 62-part request to correct her health records, to the Toronto Central Local Health Integration Network
- TCLHIN agreed to make two corrections but denied the remainder
- IPC agreed that TCLHIN was not required to make the corrections
- Most were about differences of opinion - information was not inaccurate or incomplete
- Also, consisted of good faith professional opinions
- Decision provides guidance on dealing with complicated correction requests

# No Review Where Complaint Dealt With Elsewhere

## *PHIPA* Decision 80

- An individual had concerns about the care provided to her husband at a public hospital
- Also believed that during the hospital's investigation, the doctor breached husband's privacy by speaking to a third party about his care
- Concerns raised in complaints to the hospital and the CPSO
- Health Professions Appeal and Review Board affirmed the CPSO's decision
- Unsatisfied, the individual filed a complaint with the IPC under *PHIPA*
- IPC found there was no need for a review as the matter had already been appropriately dealt with by CPSO/HPARB



# Comments to the Media – Authorized or not?

## *PHIPA* Decision 82

- A hospital responded to media requests for information about a deceased patient who had been the subject of a decision by the Health Professions Appeal and Review Board
- Patient's family complained that the hospital's statements contravened *PHIPA* by disclosing the patient's health information without consent.
- IPC found that repetition of facts about the patient, when taken from the published decision of the HPARB, is not a disclosure under *PHIPA*
- We also found that some of the hospital's statements went beyond the board decision and were considered unauthorized disclosures

# Casino Rama Investigation

- In November 2016, OLG reported to the IPC that Casino Rama Resort was subjected to a cyberattack
- IPC launched investigated the circumstances of the breach and whether reasonable security measures were in place to protect personal information of Rama customers
- The investigation revealed weaknesses in the cyber security practices – particularly with response to suspicious activity
- OLG/Casino Rama have taken steps to address the weaknesses identified – IPC satisfied
- Institutions should plan for cyberattacks by having appropriate measures in place to secure their systems and ensure early detection

# Access to Taxi Cab License Sales

## Order MO-3673

- City of Hamilton received request for specific taxi-cab license sale prices, sale dates, and license numbers associated with those sales
- City denied access, citing third party and personal privacy exemptions
- Decision: Information about sale of taxi cab licenses is not personal
- Information also not covered by exemption for third party business information

# Request for Assisted Death Records

## Order PO-3862

- Individual requested access to records held by Health Sciences North relating to requests for assisted death
- The hospital refused to confirm or deny the existence of the records on the basis that doing so would be an invasion of privacy and could compromise law enforcement activities and security at the hospital
- IPC ordered the release of the records - could not be expected to have an effect on hospital security or law enforcement and requester was not seeking access to any information that could be used to identify patients or staff

# Compelling Public Interest: Police Carding

## Order MO-3476

- Requester seeks information about street checks and racial data from Peel police
- Police deny access to six records, claiming they contain advice and recommendations
- IPC agrees that they contained advice and recommendations
- However, applies public interest override in MFIPPA (section 16)
- For most of the records, a compelling public interest in disclosure outweighs the purpose of not revealing advice and recommendations
- Order to police to disclose 5 of 6 records



What's Coming

# What We are Working On

- Reaching Out to Ontario series – Kitchener-Waterloo, May 31
- CFYSA Guide, May
- CFYSA Webinar, June 6
- Disclosure to Law Enforcement Public Fact Sheet

# Our Open Door Policy

- Any public institution or agency considering programs which may impact privacy can approach IPC for advice
- Most privacy challenges can be addressed through collaboration
- Privacy protections can be developed and can be implemented
- It is best to address privacy concerns from the outset



# 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