Notable Privacy Investigations and Consultations by Ontario's Information and Privacy Commissioner

Sherry Liang, Assistant Commissioner

Renee Barrette, Director of Policy

Information and Privacy Commissioner of Ontario

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

Presentation to Toronto Public Library - Privacy Series

May 23, 2018

Toronto Public Library Privacy Series

April 25, 2018: **Your Privacy Rights in Ontario**

- Presented by Commissioner Brian Beamish

June 20, 2018: **Cyberattacks and Digital Privacy**

- Presented by IPC staff

Agenda

- Role of the Information and Privacy Commissioner
- Notable Privacy Investigations
  - Disclosure of suicide-related information to U.S. Border Officials
  - Unauthorized access to personal health information
  - Video surveillance
  - Collection of tenants' personal information
- Notable Privacy Consultations
  - Metrolinx - Disclosing personal information to police
  - *Child, Youth and Family Services Act*
  - Smart Cities

Our Office

- The Information and Privacy Commissioner (IPC) provides independent review of government practices and decisions regarding access and privacy.
- The Commissioner is appointed by and reports to the Legislative Assembly of Ontario, to ensure impartiality.

IPC's Mandate

- *Freedom of Information and Protection of Privacy Act* (*FIPPA*)
  - Covers 300 provincial institution, including government ministries, colleges/universities, hospitals
- *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)
  - Covers 1,200 municipal organizations, including local police, school boards, public transit, municipalities
- Together, these Acts establish the public's right to access information held by public institutions, and protect personal privacy:
  - right to appeal to the IPC if access to information is denied
  - privacy complaints may be filed with the IPC

Privacy in the Private Sector

- A private sector privacy law, the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) is overseen by the Privacy Commissioner of Canada:
  - Ontario does not have its own private sector privacy law.
  - *PIPEDA* applies to commercial businesses in Ontario and throughout the country, including banks, airlines, retail stores, etc.
- Consent is a key element of *PIPEDA*:
  - Organizations are required to obtain meaningful consent for the collection, use and disclosure of personal information.
  - Consent is considered meaningful when individuals are provided with clear information explaining what organizations are doing with their information.

Privacy in the public sector: *M/FIPPA*

- *M/FIPPA* governs the collection, use and disclosure of personal information by public institutions.
- What is "personal information"
  - Information about you, where you are identifiable – contrasted with aggregated or anonymized information
  - Personal information excludes information about you in an employment or business capacity
- Unlike in the private sector, consent is not required for the government's use of personal information
- Generally, public institutions can collect personal information when it is necessary to carry out their mandates.
- Once they collect it, they have a duty to keep it safe, and not use it for extraneous purposes.
- The IPC can investigate complaints about the government's misuse of personal information.

Privacy rights are not an absolute

- Privacy is not a barrier to disclosure where the public interest requires transparency.
- Situations where disclosure of personal information is permitted include:
  - Compelling circumstances affecting health and safety
  - Disclosure to comply with a warrant
  - Duty to report child abuse or neglect

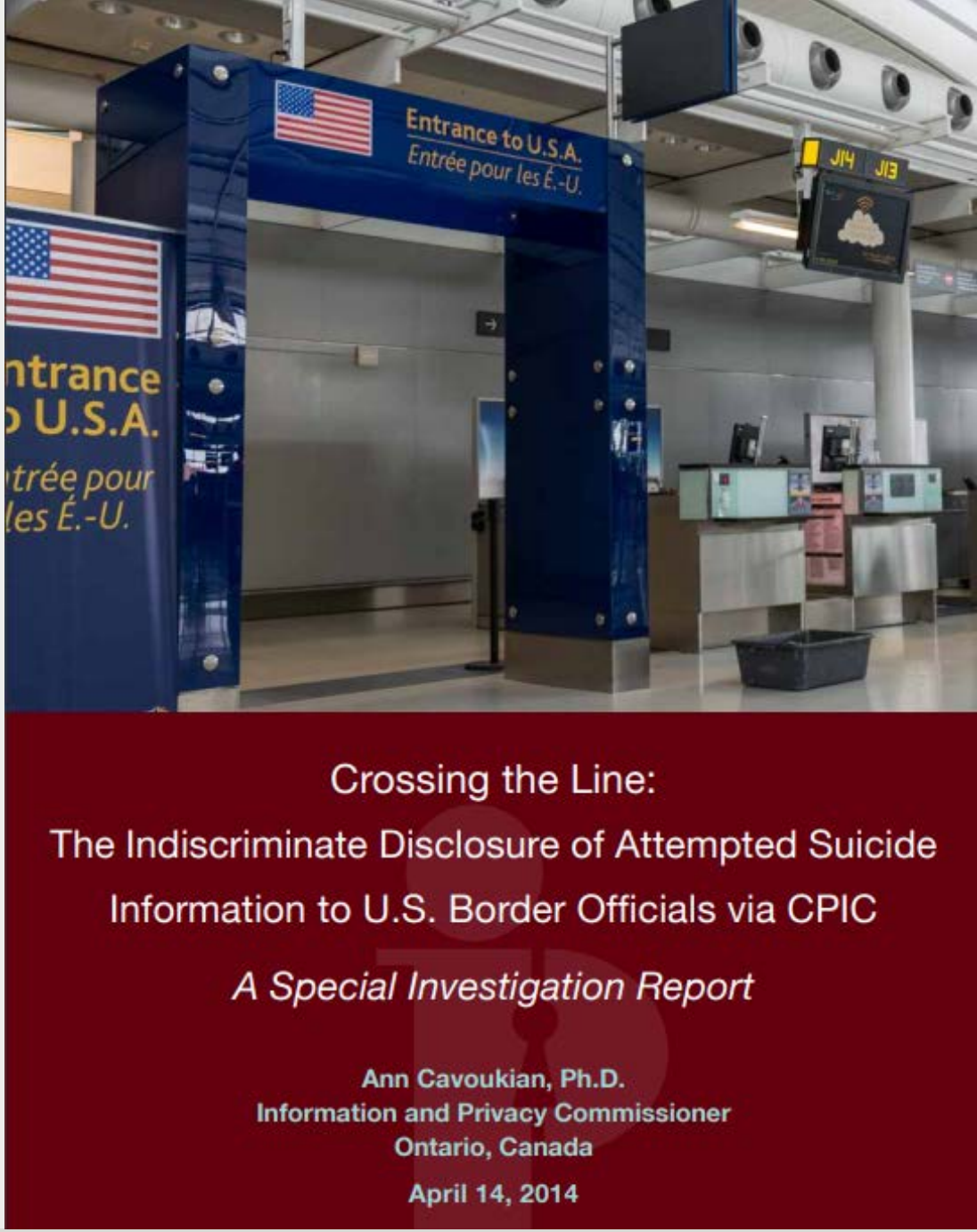
Health privacy and new mandates

- *Personal Health Information Protection Act* (*PHIPA*):
  - Covers individuals and organizations involved in the delivery of health care services, including doctors, pharmacists, hospitals, health clinics
  - Includes comprehensive privacy protections for personal health information
  - Patients have a right of access to their health information, right to appeal to the IPC
- The IPC's mandate is expanding:
  - *Child, Youth and Family Services Act*
  - *Anti-Racism Act*

Notable Privacy Investigations

Suicide-related disclosures to U.S. Border Officials

- The IPC investigated complaints from several Ontarians who were denied entry into the United States, apparently on the basis of their mental health history.
- IPC discovered that some police services were sharing information about attempted suicides via the Canadian Police Information Centre (CPIC), a national law enforcement database.
- U.S border officials have access to CPIC and were relying on this information to deny entry into the country.



Cont'd

Suicide-related disclosures to U.S. Border Officials

- The IPC could not tell U.S. Border Officials what to do or not do.
- But it could look at whether Ontario police should be putting that kind of information into CPIC.
- The IPC recommended that police look at four factors to justify putting suicide-related information into CPIC:
    - threat of serious violence or harm to others;
    - intentional provocation of a lethal response by the police;
    - history of serious violence or harm to others; or
    - suicide attempt while in police custody.

Cont'd

Suicide-related disclosures to U.S. Border Officials

- Most police services we consulted agreed to implement the IPC's recommendations.
- Toronto Police Service initially refused to change its practice of sharing information via CPIC about *all* attempted suicides, regardless of the circumstances.
- The IPC started a legal action against the Toronto Police Service which resolved when the TPS agreed to new procedures that met our concerns.

Unauthorized Access to Personal Health Information

- While the vast majority of health workers understand and respect patient privacy, some take advantage of their access to electronic records to snoop into patients' personal health information.
- IPC has investigated a number of these cases. Motivations for snooping include:
  - Interpersonal conflicts
  - Curiosity
  - Monetary gain
- Impact of snooping on patients can include psychological harm and a loss of trust in the health system.

Cont'd

Unauthorized Access to Personal Health Information

- The Rouge Valley Health System reported two privacy breaches to the IPC. Both involved hospital employees who accessed the electronic medical records of new mothers for the purpose of marketing RESPs.
- The IPC learned that the hospital was unable to fully audit how information was being accessed, due to technical limitations.
- The gaps in the hospital's auditing capabilities meant it could not adequately protect patient information.

Unauthorized Access to Personal Health Information

- The IPC issued Health Order-013, requiring the Rouge Valley hospital to change its electronic information systems to ensure the ability to audit all instances of access to personal health information.
- This order, like all IPC orders, is publicly available on our website at www.ipc.on.ca

Cont'd

Unauthorized Access to Personal Health Information

- The hospital **appealed** the IPC's Order to the Divisional Court.
  - However, after discussion with the IPC, the hospital withdrew its appeal.
- Hospital and IPC cooperated on strategies and a **work plan** to implement the Order relating to auditing of electronic information systems:
  - IPC and hospital agreed on the systems to be upgraded with logging/auditing functionality.
  - Systems were upgraded unless:
    - system was to be retired,
    - limited staff had access, or
    - system only conducted real-time monitoring and did not record personal health information.

Video surveillance

- The IPC has conducted several investigations of video surveillance programs at schools.
- These investigations looked at whether
  - Installing the cameras was necessary to the operations of the schools – did the board assess the need for the cameras or install them without thought?
    - IPC recommended one school board conduct an assessment of the need for the cameras.
  - Cameras installed outside of school buildings had an impact on the privacy of surrounding neighbours.
    - IPC recommended that the board ensure the cameras not capture images from neighbouring properties

Cont'd

Video surveillance

- 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.
- The IPC decided the program and the expansion were justified. The IPC's policy department worked with the police to make sure the details of the surveillance complied with privacy best practices. For further information about the best practices, see our guidelines and fact sheet.

Cont'd

Video surveillance

- In February 2018, Hamilton City Council voted to consider amending its policy to permit cameras on private property to conduct video surveillance of public spaces, for use by the police.
- Our office does not regulate the use of video cameras by private citizens.
- But we have oversight over the actions of council that could undermine privacy rights under *MFIPPA*.
- Commissioner Brian Beamish wrote to Hamilton's mayor and police chief expressing concern about the proposal.
- His message: the city and the police should not encourage homeowners to monitor public spaces through their home surveillance cameras.

Collection of Tenants' Personal Information

- When landlords collect information from tenants, they must comply with Canada's private sector privacy law, *PIPEDA*.
  - The federal privacy commissioner has oversight and offers guidance on its website:
    - www.priv.gc.ca/en/privacy-topics/landlords-and-tenants/privacy-in-the-landlord-and-tenant-relationship

- When municipalities collect tenants' information, they must comply with *MFIPPA*.
  - IPC has oversight
  - The municipality has an obligation under *MFIPPA* to protect the privacy of the information.

Cont'd

Collection of Tenants' Personal Information

- In 2014, the IPC investigated a city that passed a by-law requiring landlords to supply names, phone numbers and other personal information of tenants, as part of its landlord licensing process.
- The IPC questioned why this tenant information was needed in order to license landlords.
- The city agreed to amend its by-law to stop collecting this information.
- It also agreed to destroy the personal information it had collected.

How to make a Privacy Complaint

Government-Held Records

- Contact institution's Freedom of Information and Privacy Coordinator and try to resolve your concern
- If not satisfied, file a complaint with our office by writing a letter or completing a Privacy Complaint form

Health Records

- Contact the health care provider and attempt to resolve the matter
- If not resolved, file a privacy complaint with our office within 12 months

Notable Privacy Consultations

IPC's Policy Role

- Engage in research into matters affecting access and privacy.
- Comment on proposed legislation or government programs.
- Educate the public and stakeholders about access and privacy laws and issues, through research, publications and public speaking.
- Develop guidance to help institutions understand their legislative obligations, and help the public understand their access and privacy rights.

Metrolinx disclosing personal information to police

- In June 2017, the Toronto Star reported that Metrolinx had been "quietly sharing Presto users' information with police".
- The Star reported that:
  - Metrolinx has received 26 requests from police over the previous five months, 12 of which it had granted.
  - The requests related to alleged criminal offences and missing persons cases.

Cont'd

Metrolinx disclosing personal information to police

- Metrolinx committed to revising its privacy policy following the Toronto Star investigation.
- Metrolinx legal and privacy team consulted with the IPC during the review of their new policy.

Cont'd

Metrolinx disclosing personal information to police

- Ontario's public sector privacy law permits:
  - disclosure to comply with a court order or warrant.
  - disclosure of personal information to a law enforcement agency *without* a warrant, if:
    - disclosure is to an institution or a law enforcement agency in Canada,
    - the disclosure is to aid an investigation, and
    - the investigation is undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result.
  - proactive disclosure by institutions.

Cont'd

Metrolinx disclosing personal information to police

- Best practices for disclosure to police:
  1. Generally insist on a warrant
  2. In urgent circumstances (e.g., missing person), an institution may exercise its discretion to disclose without a warrant, if disclosure is to aid an investigation *and*:
     - A specific request was received from police in the context of a specific law enforcement proceeding
     - The institution exercises its discretion based on an independent and informed judgement
  3. Police must provide badge number, contact information, description of law enforcement proceeding, file number, etc.
  4. Institutions should only disclose proactively if there is reasonable basis to believe an offence has occurred
     - Disclosure should be limited to that which is relevant and necessary

Child, Youth and Family Services Act (CYFSA)

- The *CYFSA* applies to child and family services providers such as children's aid societies, foster and group homes and programs for at-risk youth.
- Part X of the *CYFSA* will become effective January 1, 2020. Part X:
  - establishes new rights for individuals to access their personal information from service providers, and request corrections;
  - sets out new privacy rules for the collection, use and disclosure of personal information by service providers;
  - establishes the IPC as the oversight body for Part X. The IPC can hear privacy and access complaints and make orders.

Cont'd

Child, Youth and Family Services Act

- The IPC has been recommending over the past fifteen years that children's aid societies should be subject to privacy legislation.
- The IPC was consulted extensively by the government in the development of this new legislation.
- Part X of the *CYFSA* represents a big step forward for Ontario's child and youth sectors:
  - closes a legislative gap for privacy rights;
  - promotes accountability.

Cont'd

Child, Youth and Family Services Act

- Strengths of the *CYFSA* (Part X) include:
  - consent-based framework
  - individuals' right of access to their :
    - within 30 days, with possible 90 day extension
    - no fees can be charged for access
  - mandatory privacy breach reporting
  - clear offense provisions
  - adequate powers for IPC to ensure that complaints are properly reviewed
  - facilitates consistency among service providers' information practices

Smart Cities

- "Smart cities" are communities that use connected technologies to collect and analyze data in order to improve services for citizens.
  - Examples include:
    - sensors that dim streetlights when no one is around
    - real-time parking apps that map out nearest available spots
    - garbage cans that send a signal when full

Cont'd

Smart Cities

- Smart cities have lots of potential, but require robust privacy protections.
- Safeguards are necessary to ensure that personal information is not compromised, and that data collected is de-identified and made publicly available as open data.
- Personal information should not be:
  - used to track people as they go about their daily activities (surveillance),
  - used for another purpose, unbeknownst to the individuals (scope creep)

Cont'd

Smart Cities

- Privacy protections and controls:
  - Data Minimization:
    - Only collect, use and disclose personal information where it is necessary
  - Community Engagement and Project Transparency
  - Privacy Impact Assessment and Threat Risk Assessment
  - Data Governance:
    - Decide who will hold the data and who will be accountable for privacy
    - Ensure privacy requirements are set out in contracts
  - Consent
  - De-identification
    - De-identify personal information at earliest opportunity; Guard against re-identification
    - Only retain, use and disclose de-identified information

Smart Cities

- IPC released smart cities guidance in April 2018, to raise **public awareness** about privacy risks.
- We are raising **institutional awareness** through public presentations at conferences and by engaging directly with organizations involved in smart cities projects.

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

Cont'd

Smart Cities Outreach

- IPC is working with other privacy regulators to provide advice to the federal government on a program that will fund select smart city projects.
- Our goal is to help ensure that funding is only provided to projects that have built in privacy protection.

Smart Cities Outreach

- Sidewalk Labs and Waterfront Toronto have signed a deal to partner on a new smart city development.
  - If it goes ahead, "Sidewalk Toronto" would represent North America's largest smart city project.
- Waterfront Toronto has committed to engaging with the IPC:
  - The IPC, along with the federal privacy commissioner and all three levels of government, will be invited to participate in meetings of the Digital Strategy Advisory Panel.

Cont'd

IPC Guidance Materials for the Public

- Guidance materials for the public are available on our website (www.IPC.on.ca), including:
  - *M/FIPPA* Mini Guides
  - Your Rights under Ontario's Freedom of Information Laws
  - Identity Theft: A Crime of Opportunity
  - Making an Access Request to a Police Service
  - Your Health Information: Your Access and Correction Rights
  - Fact Sheet: What is Personal Information
  - *PHIPA* and Your Privacy
  - What Students Need to Know about Freedom of Information and Protection of Privacy
  - Big Data and Your Privacy Rights

HOW TO 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