

Your Access and Privacy Rights in Ontario

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

Lifelong Learning
Niagara

May 23, 2018

Ontario's Access and Privacy Laws

- *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*

Ontarians' Access and Privacy Rights

- Right to file freedom of information (FOI) requests
- Right to appeal FOI decisions
- Right of access to their personal health information
- Right to file privacy complaints

Personal Information Protection and Electronic Documents Act (PIPEDA)

- Federal legislation
- Promotes consumer trust in electronic commerce
- Governs how private sector organizations collect, use and disclose personal information
- Covers personal information collected by organizations that do not come under Ontario's access and privacy laws

Our Office

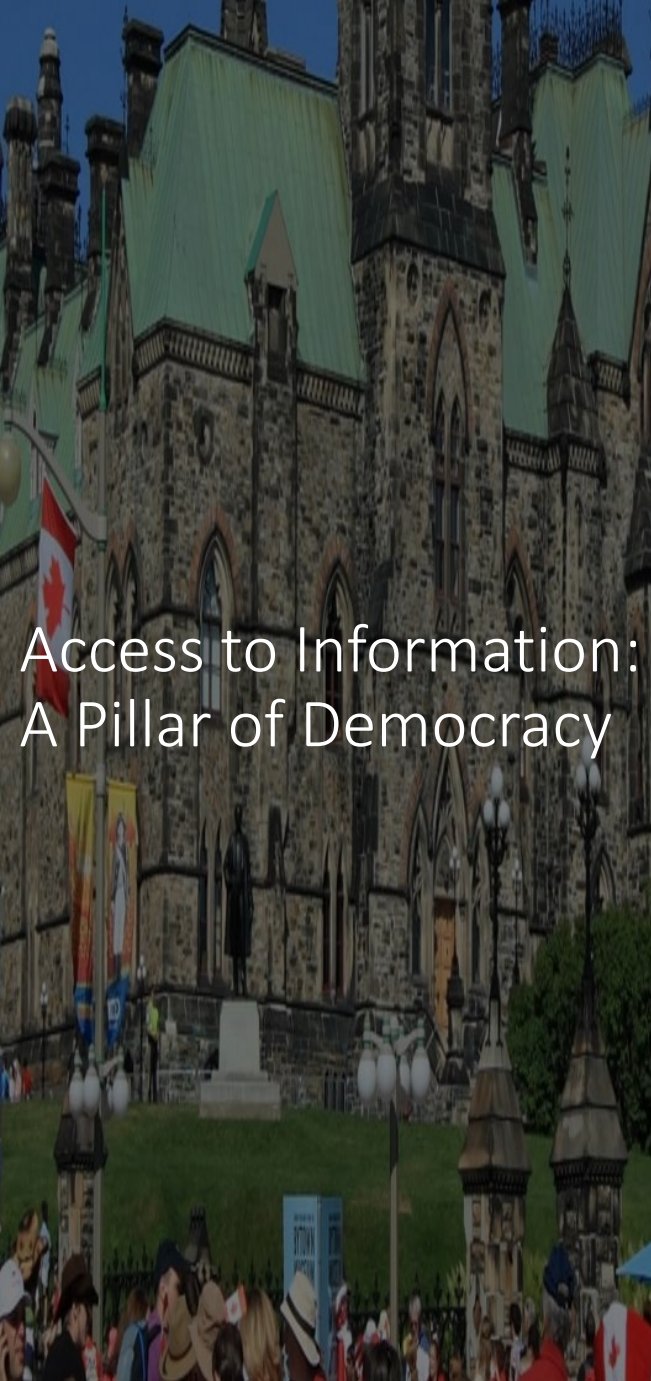
- Information and Privacy Commissioner (IPC) of Ontario provides **independent** review of government decisions and practices on access and privacy
- Commissioner appointed by, and reports to the Legislative Assembly, to ensure **impartiality**

Our Mandate

- *Resolve* access to information appeals
- *Investigate* privacy complaints – public sector and health
- *Research* access and privacy issues
- *Comment* on proposed government legislation and programs
- *Educate* the public on issues of access and privacy

Access





Access to Information: A Pillar of 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

“The overarching purpose of access to information legislation ... is to facilitate democracy.”

Justice La Forest

Dagg v. Canada (Minister of Finance), 1997

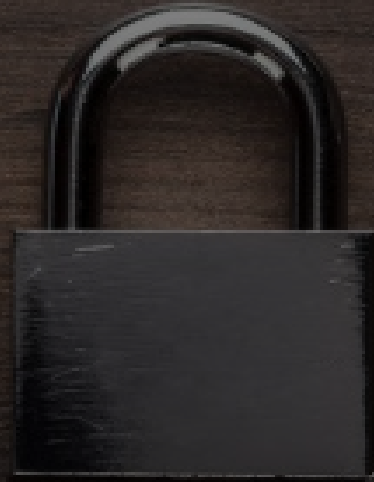
Freedom of Information Requests

1. Determine which institution has the information
2. Write a formal letter, or use one of our forms, requesting the information
3. Send request to the Freedom of Information Coordinator, with \$5.00 fee
 - Response within 30 days
 - If denied, institution must give written notice with reasons
 - You may file an appeal with our office

Right of Appeal

- **Who may appeal to the Commissioner?**
 - the requester or an affected person
- **Types of appeals:**
 - fees
 - exemption claims
 - exclusion claims
 - custody or control question
 - time extension or failure to issue decision
 - whether search was adequate

Privacy



Fair Information Practices

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure, Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

What is Personal Information?

- Recorded information about you
- Name, address, sex, age, education, and medical or employment history
- Social Insurance Number
- Personal views or opinions
- Business information is not personal information



What is Personal Information?

October 2016

INTRODUCTION

The *Freedom of Information and Protection of Privacy Act (FIPPA)* and the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* (the acts) protect the privacy of personal information while providing individuals with a right of access to their own information.

In this fact sheet, we provide guidance about how the Information and Privacy Commissioner (IPC) interprets the term “personal information.”

HOW IS PERSONAL INFORMATION DEFINED IN THE ACTS?

The acts define personal information as “recorded information about an identifiable individual,” and include a list of examples of personal information (see Appendix A for the full definition).

Recorded information

Information can be recorded in any format, such as paper records, electronic records, digital photographs, videos or maps.

About an identifiable individual

Information is about an identifiable individual if:

- it is about the individual in a personal capacity; that is, it reveals something of a personal nature about the individual, and
- it is reasonable to expect that an individual can be identified from the information (either alone or by combining it with other information)

The listed examples include a person’s name when combined with other information about them, such as their address, sex, age, education, or medical history. These examples are not exhaustive and many other kinds of information may still qualify as personal information.

Your Privacy Rights

- Public institutions must protect personal information and follow specific rules on how they collect, use, retain, disclose and dispose of it
- Your personal information will only be collected, used or disclosed for legitimate, limited and specific purposes
- Institutions must tell you how they intend to use your information
- You may file privacy complaints with the IPC

PHIPA

Gives you the right to:

- be informed why your personal health information is being collected, used or disclosed
- be notified of the theft, loss or unauthorized use
- either refuse or give consent to the collection, use or disclosure of PHI
- withdraw consent or instruct that your PHI not be used or disclosed without your consent
- access health records
- request corrections to health records
- complain to our office if refused access your health records, refused a correction request, or if information is compromised
- begin court proceedings for harm suffered due to an offence under *PHIPA*

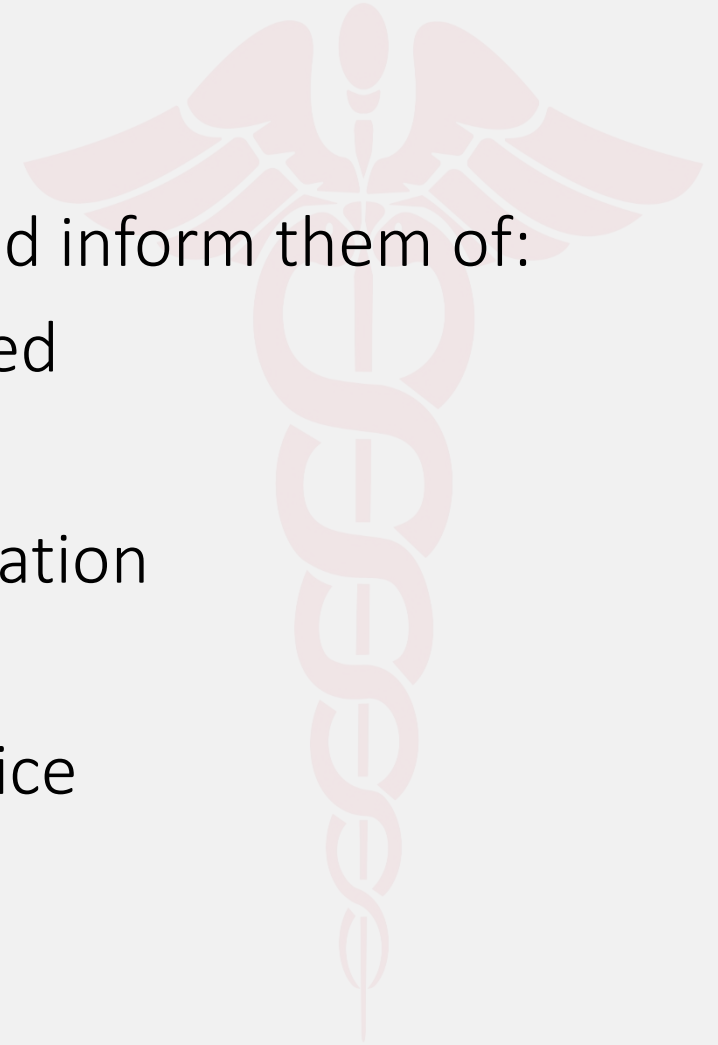
Access or Correction of Health Records

- Contact health care provider directly
- You may need to make request in writing, or use IPC form
- Health care provider may charge a fee to access records, but not to correct
- You should receive a response from 30 to 60 days
- If denied access or correction, you may file an appeal with the IPC

Health Privacy Breach Notification

Health care providers must notify affected individuals and inform them of:

- extent of the breach and kind of information involved
- steps taken to rectify the breach
- who to contact for assistance and additional information
- whether they have contacted our office
- the individual's right to file a complaint with our office



Privacy and Personal Health Information in Ontario

- Health care providers must notify our office of a privacy breach when:
 - personal health information is accessed without authorization
 - personal health information is lost or stolen
 - further use or disclosure without authority after a breach
 - pattern of breaches
 - disciplinary action is taken
 - a breach is determined as being “significant”

Privacy and Your Health Card

- Only individuals or institutions providing health care may **require you** to present your health card
- Some organizations, such as insurance companies, may ask for health card, but it is voluntary and the information can only be used for health care
- Organizations not involved in provincially-funded health care may not collect, record, or use health cards for ID purposes
- It is your decision whether to show health card for non-health care related ID
- Be prudent when showing health card

Era of “Big Data”

More personal information is created and shared online

- Web browsing
- Email
- Instant messaging
- Social media
- Cloud storage

More personal information is created, stored and transmitted by

- Personal computers
- Smartphones
- Watches / fitbits
- Vehicles
- Homes (thermostats, meters)

Privacy Risks

Cont'd

Risks to Personal Information

- Overcollection and retention
- Loss and destruction
- Unauthorized disclosures and uses
 - Interception
 - Hacking
 - Snooping employee
 - Human error

Impacts on Individuals

- Surveillance and profiling
- Discrimination and denial of service
- Identity theft and fraud
- Harm and embarrassment
- Loss of trust

A Breach of Privacy is a Breach of Trust

- Proper stewardship of personal information collected by institutions is fundamental to maintaining the public's trust and confidence
- Disclosure of your personal information by an institution is not permitted except in specific circumstances

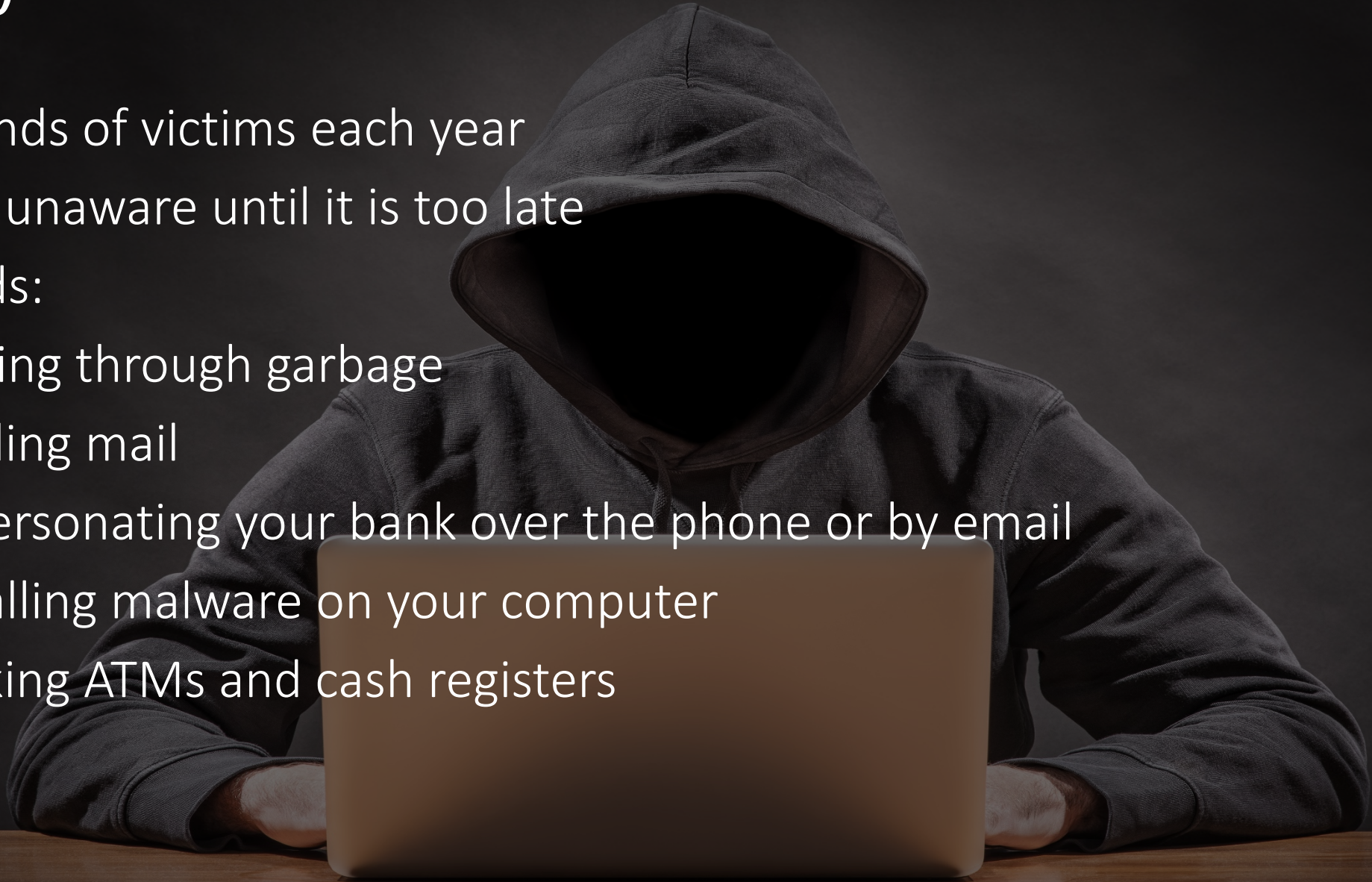
Facebook Data Scandal

What happened?

- Facebook let academic researchers obtain psychological profiles on 300,000 FB users through a quiz app called *thisisyourdigitallife*
- researchers collected users' "social graph" data, and also from 87 million friends -- including more than 600 thousand Canadians
- shared data included names, profile information, likes, comments, shares, and more
- instead of deleting data, researchers gave to private companies who matched with other data sources to create detailed "psychographic" profiles of users
- detailed profiles were allegedly used to "micro-target" voters and to influence the Brexit referendum and US election results
- investigations and lawsuits are now underway around the world, including by privacy authorities in Canada, the U.S. and the U.K.

Identity Theft

- Thousands of victims each year
- Victims unaware until it is too late
- Methods:
 - looking through garbage
 - stealing mail
 - impersonating your bank over the phone or by email
 - installing malware on your computer
 - hacking ATMs and cash registers



Minimize Risk of Identity Theft

Limit Exposure

- have someone collect your mail while you are away
- carry only essential ID, leave SIN card at home
- minimize amount of personal information shared online and on the phone
- Use security settings on computers and mobile phone
- Securely dispose of personal information – **Do Not** throw it in the garbage

Stay Secure

- Securely store sensitive documents
- Use strong passwords
- Keep security software up-to-date (antivirus, anti-spyware, firewall)

Act

- Review bills and bank statements
- Review credit report every year
- **Do not** reply to suspicious emails or texts

Phishing

Tricking individuals into disclosing personal or sensitive information through deceptive computer-based means, such as fake emails and web sites

What should you do?

- Understand and look for the signs of fraudulent emails and web sites
- Never reply to email requests for financial or personal information
Instead, contact the person or organization through a separate channel
- Do not provide passwords, PINs or other access codes in response to emails or pop up windows
Only enter such information into the legitimate web site or application
- Do not open suspicious email file attachments, even if they come from known senders
Contact the sender to confirm the unexpected attachment is legitimate
- Use anti-phishing software

Protect Yourself Online

Best Practices

- Stay aware and informed
- Beware of “free” apps and services
- Use privacy-friendly services and technologies
- Check your privacy settings and preferences
- Do not reuse passwords
- Securely dispose of computing devices
- Access and delete your personal information

Report Loss or Theft of Personal Information

- If your driver's licence, OHIP card or other provincial ID is lost or stolen, contact ServiceOntario
- If a provincial institution mishandles your personal information, contact our office
- If your personal information has been mishandled by a commercial business or a federal institution, contact the federal privacy commissioner
- Identity theft is a criminal matter and can also be reported to the police

Privacy Complaints

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

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 Ontario government website's 'Public sector salary disclosure' page. At the top, there is the Ontario logo, a search bar, and navigation links for 'français' and 'MENU'. The main heading is 'Public sector salary disclosure', followed by a brief description: 'The names, positions, salaries and total taxable benefits of public sector employees paid \$100,000 or more in a calendar year.' Below this is a blue button labeled 'Search the 2017 disclosure'. To the right, a 'Related' section contains a link to 'Public sector salary disclosure background and FAQ'. Under 'On this page', there are two numbered links: '1. Public sector salary disclosure for 1996 to 2017' and '2. Guide and forms for 2018 (disclosure for 2017)'. At the bottom, a paragraph explains the 'Public Sector Salary Disclosure Act, 1996'.

The screenshot shows the Ontario government website's 'Travel, meal and hospitality expenses' page. The header includes the Ontario logo, a search bar with 'Search Ontario.ca', and navigation links for 'contact us | français' and 'Topics +'. The main heading is 'Travel, meal and hospitality expenses', with a sub-heading: 'Browse or search work-related expenses claimed by government employees, elected officials and political staff.' Below this, there are instructions on how to use the 'Show/hide columns' button and how to sort and filter the information. A link to 'Learn more about the rules covering these expenses.' is provided. The page features a section titled 'View expenses by fiscal year' with a dropdown menu set to '2014-2015'. Below this is a search interface with a search bar, dropdowns for 'All staff' and 'All months', and a 'Show/hide columns' button. A table of checkboxes allows users to select which columns to display in the results, including 'Show default', 'Ministry', 'Destination', 'Other Transportation', 'Subtotal', 'Name', 'Purpose', 'Attendees', 'Accommodation', 'Hospitality', 'Title', 'Start Date', 'Other Attendees', 'Meals', 'Other Expenses', 'Type', 'End Date', 'Air Fare', 'Incidentals', and 'Total'.

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.



[Segment Name]	[Segment Name]	[Segment Name]
52,500.00	\$30,000.00	\$58,750.00
0,000.00	\$95,000.00	\$70,000.00
,000.00	\$12,500.00	\$27,500.00
333.33)	(\$13,500.00)	\$35,000.00

Algoma Public Health

Growing understanding by institutions of the importance of the public interest override.



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.



Jeffrey Baldwin Inquest



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

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

- 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;



Alberta Association of Chiefs of Police's Homicide Victims Policy

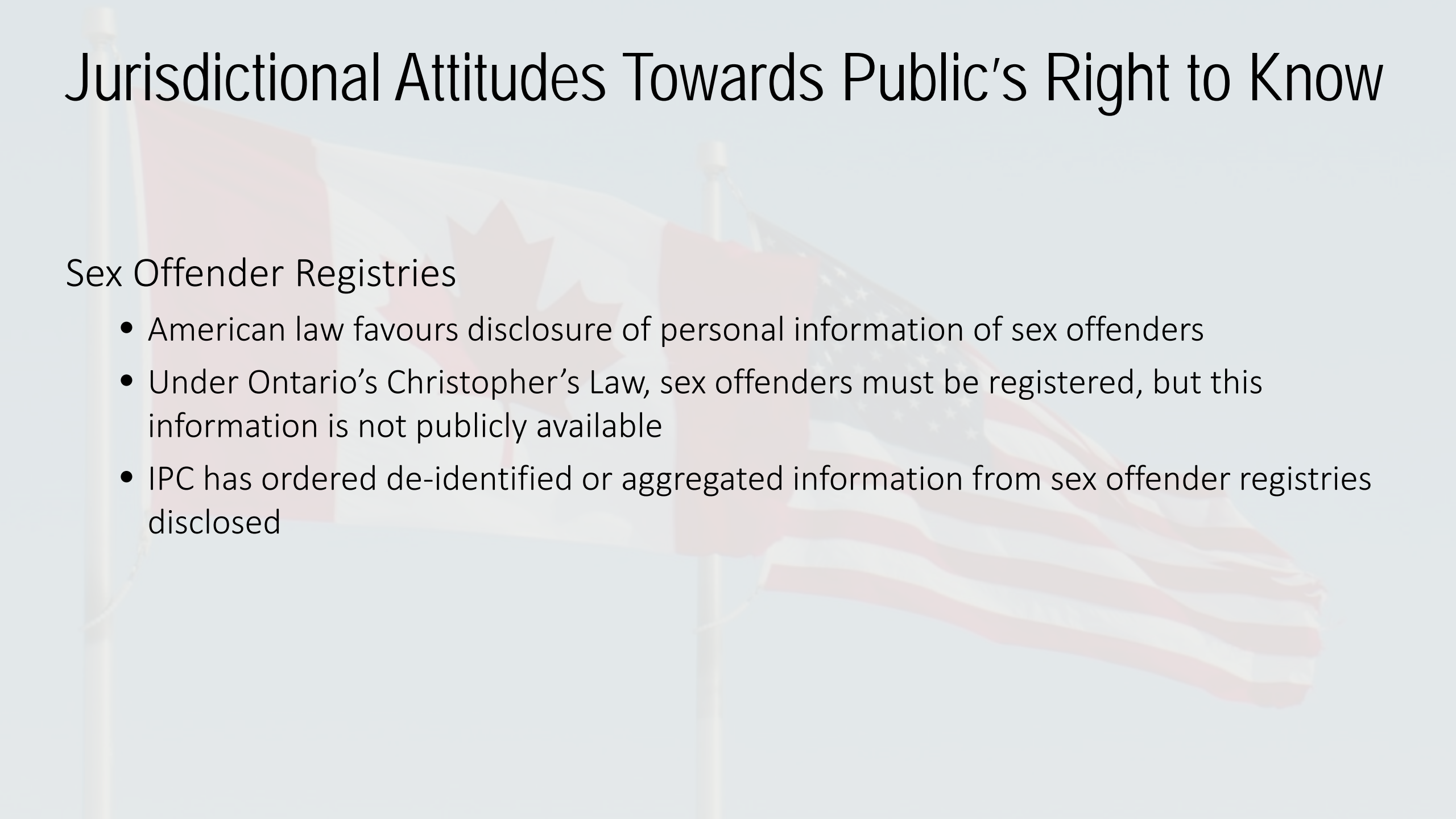
New rules work to strike an appropriate balance between protecting the privacy of homicide victims and the public's right to know.

Jurisdictional Attitudes Towards Public's Right to Know

American vs. Canadian expectations about public disclosure of politicians' health status



Jurisdictional Attitudes Towards Public's Right to Know



Sex Offender Registries

- American law favours disclosure of personal information of sex offenders
- Under Ontario's Christopher's Law, sex offenders must be registered, but this information is not publicly available
- IPC has ordered de-identified or aggregated information from sex offender registries disclosed



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*

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