Latest Developments in Access and Privacy at 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

MGCS Access and Privacy Forum

June 11, 2018

Smart Cities

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

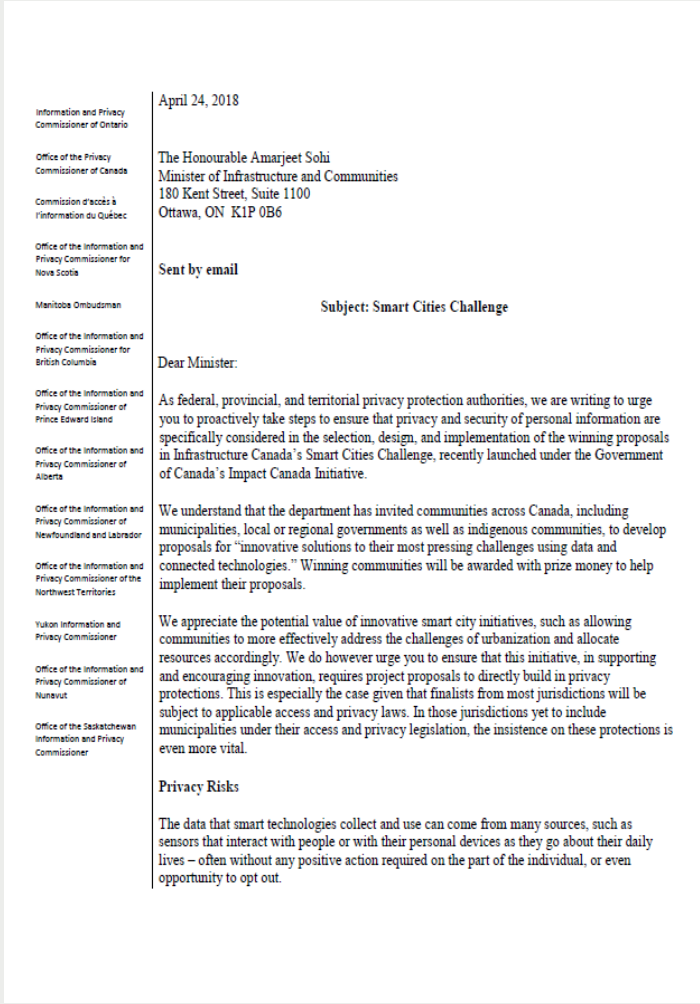
Cont'd

- 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: Top 20 Finalists

Cont'd

- Biigtigong Nishnaabeg (Pic River First Nation), Ontario
- Cree Nation of Eastmain, Quebec
- Bridgewater, Nova Scotia
- Mohawk Council of Akwesasne, Quebec
- Yellowknife, Northwest Territories
- The Pas, Opaskwayak Cree Nation, Rural Municipality of Kelsey, Manitoba
- Côte Saint-Luc, Quebec
- Nunavut Communities, Nunavut
- Fredericton and Saint Mary's First Nation, New Brunswick
- Parkland, Brazeau, Lac Ste Anne and Yellowhead Counties, Alberta
- Airdrie and Area, Alberta
- Richmond, British Columbia
- City of Guelph and Wellington County, Ontario
- Saskatoon, Saskatchewan
- Greater Victoria, British Columbia
- Region of Waterloo, Ontario
- Quebec City, Quebec
- Edmonton, Alberta
- Surrey and Vancouver, British Columbia
- Montréal, Quebec



Information and Privacy Commissioner of Ontario

Office of the Privacy Commissioner of Canada

Commission d'accès à l'information du Québec

Office of the Information and Privacy Commissioner for Nova Scotia

Manitoba Ombudsman

Office of the Information and Privacy Commissioner for British Columbia

Office of the Information and Privacy Commissioner of Prince Edward Island

Office of the Information and Privacy Commissioner of Alberta

Office of the Information and Privacy Commissioner of Newfoundland and Labrador

Office of the Information and Privacy Commissioner of the Northwest Territories

Yukon Information and Privacy Commissioner

Office of the Information and Privacy Commissioner of Nunavut

Office of the Saskatchewan Information and Privacy Commissioner

April 24, 2018

The Honourable Amarjeet Sohi
Minister of Infrastructure and Communities
180 Kent Street, Suite 1100
Ottawa, ON K1P 0B6

Sent by email

Subject: Smart Cities Challenge

Dear Minister:

As federal, provincial, and territorial privacy protection authorities, we are writing to urge you to proactively take steps to ensure that privacy and security of personal information are specifically considered in the selection, design, and implementation of the winning proposals in Infrastructure Canada's Smart Cities Challenge, recently launched under the Government of Canada's Impact Canada Initiative.

We understand that the department has invited communities across Canada, including municipalities, local or regional governments as well as indigenous communities, to develop proposals for "innovative solutions to their most pressing challenges using data and connected technologies." Winning communities will be awarded with prize money to help implement their proposals.

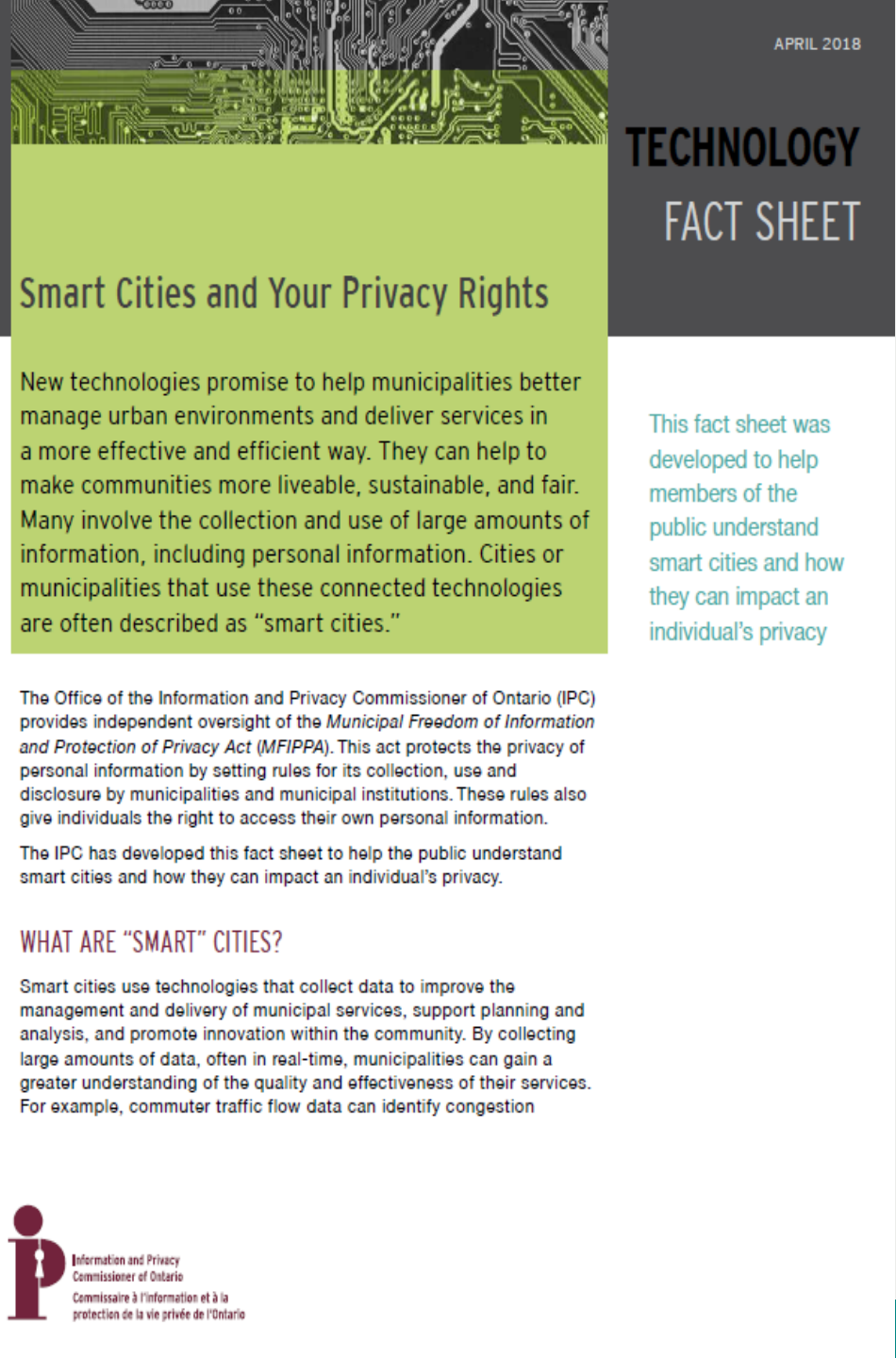
We appreciate the potential value of innovative smart city initiatives, such as allowing communities to more effectively address the challenges of urbanization and allocate resources accordingly. We do however urge you to ensure that this initiative, in supporting and encouraging innovation, requires project proposals to directly build in privacy protections. This is especially the case given that finalists from most jurisdictions will be subject to applicable access and privacy laws. In those jurisdictions yet to include municipalities under their access and privacy legislation, the insistence on these protections is even more vital.

Privacy Risks

The data that smart technologies collect and use can come from many sources, such as sensors that interact with people or with their personal devices as they go about their daily lives – often without any positive action required on the part of the individual, or even opportunity to opt out.

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



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.

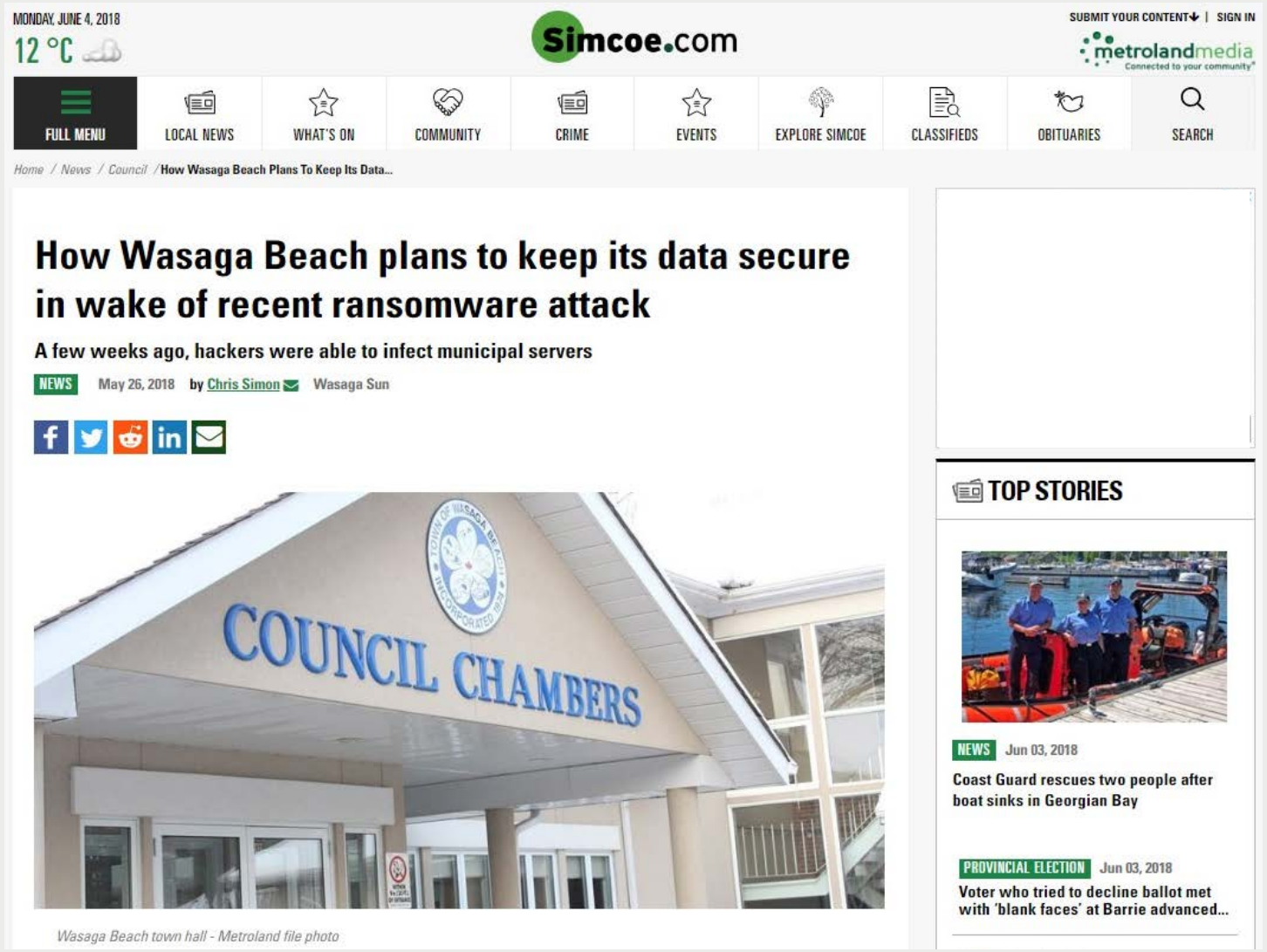
WHAT ARE "SMART" CITIES?

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

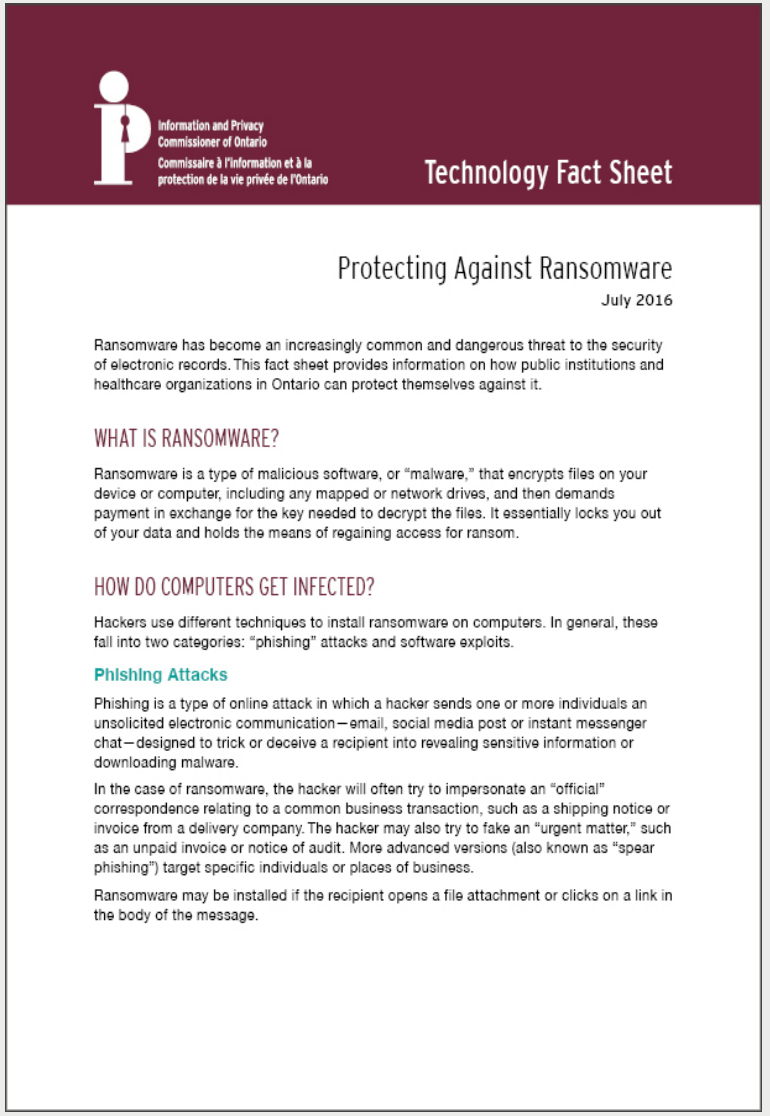
Wasaga Beach Ransomware Attack

- Hackers infected the town's servers with a code that locked staff out of files and data, including the personal tax information of residents
- The town payed the ransom to regain access to its servers
- The town has since installed a secure offsite backup that will protect the municipality's computer data



Protecting Against Ransomware

- Only download email attachments or click on links from trusted sources
- Avoid opening unsolicited email attachments
- Back-up all records regularly and check to ensure data is saved
- Ensure automatic update of security software and anti-virus programs
- Security software should receive automatic notices and perform real-time scans



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

Technology Fact Sheet

Protecting Against Ransomware

July 2016

Ransomware has become an increasingly common and dangerous threat to the security of electronic records. This fact sheet provides information on how public institutions and healthcare organizations in Ontario can protect themselves against it.

WHAT IS RANSOMWARE?

Ransomware is a type of malicious software, or "malware," that encrypts files on your device or computer, including any mapped or network drives, and then demands payment in exchange for the key needed to decrypt the files. It essentially locks you out of your data and holds the means of regaining access for ransom.

HOW DO COMPUTERS GET INFECTED?

Hackers use different techniques to install ransomware on computers. In general, these fall into two categories: "phishing" attacks and software exploits.

Phishing Attacks

Phishing is a type of online attack in which a hacker sends one or more individuals an unsolicited electronic communication—email, social media post or instant messenger chat—designed to trick or deceive a recipient into revealing sensitive information or downloading malware.

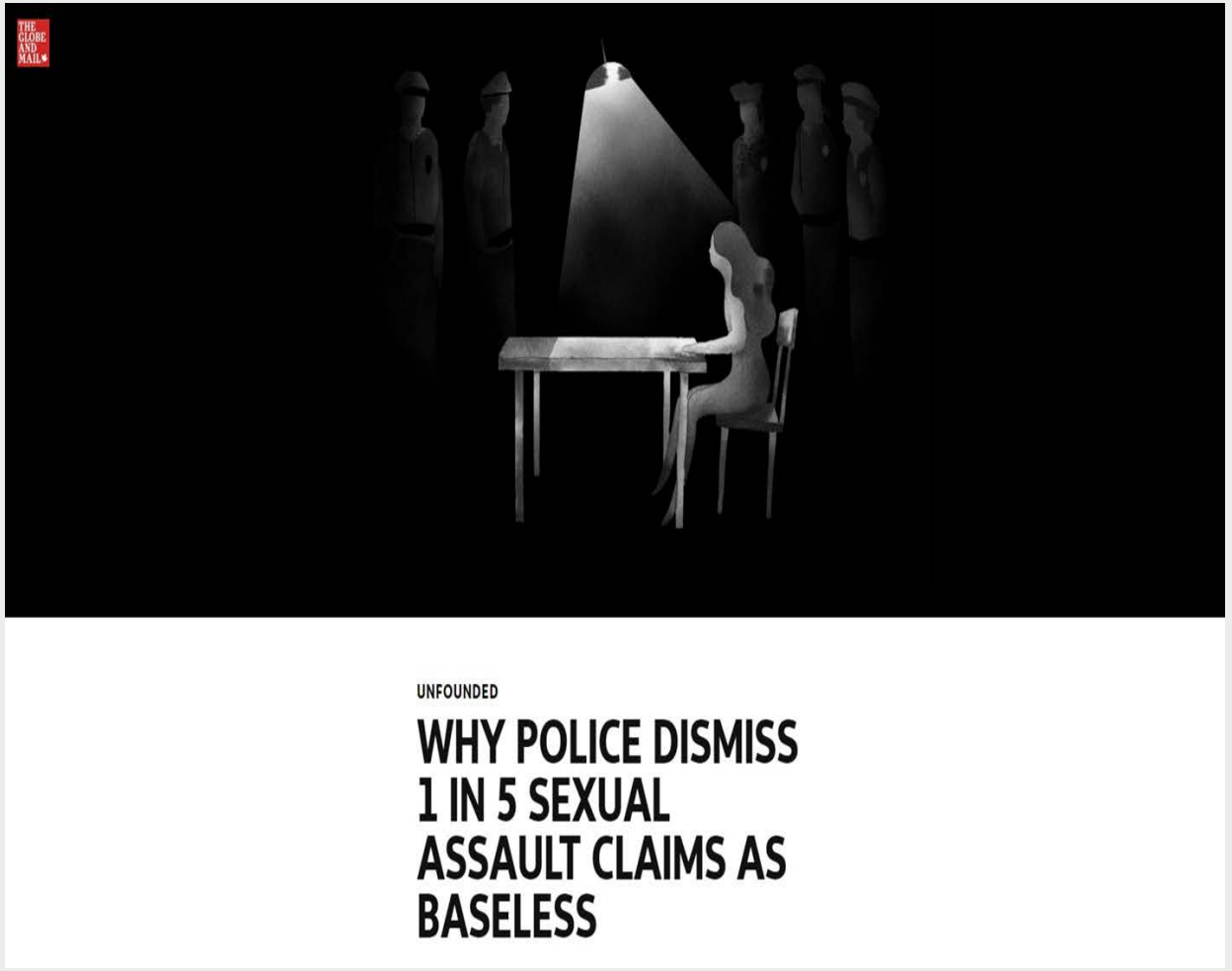
In the case of ransomware, the hacker will often try to impersonate an "official" correspondence relating to a common business transaction, such as a shipping notice or invoice from a delivery company. The hacker may also try to fake an "urgent matter," such as an unpaid invoice or notice of audit. More advanced versions (also known as "spear phishing") target specific individuals or places of business.

Ransomware may be installed if the recipient opens a file attachment or clicks on a link in the body of the message.

Policing

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

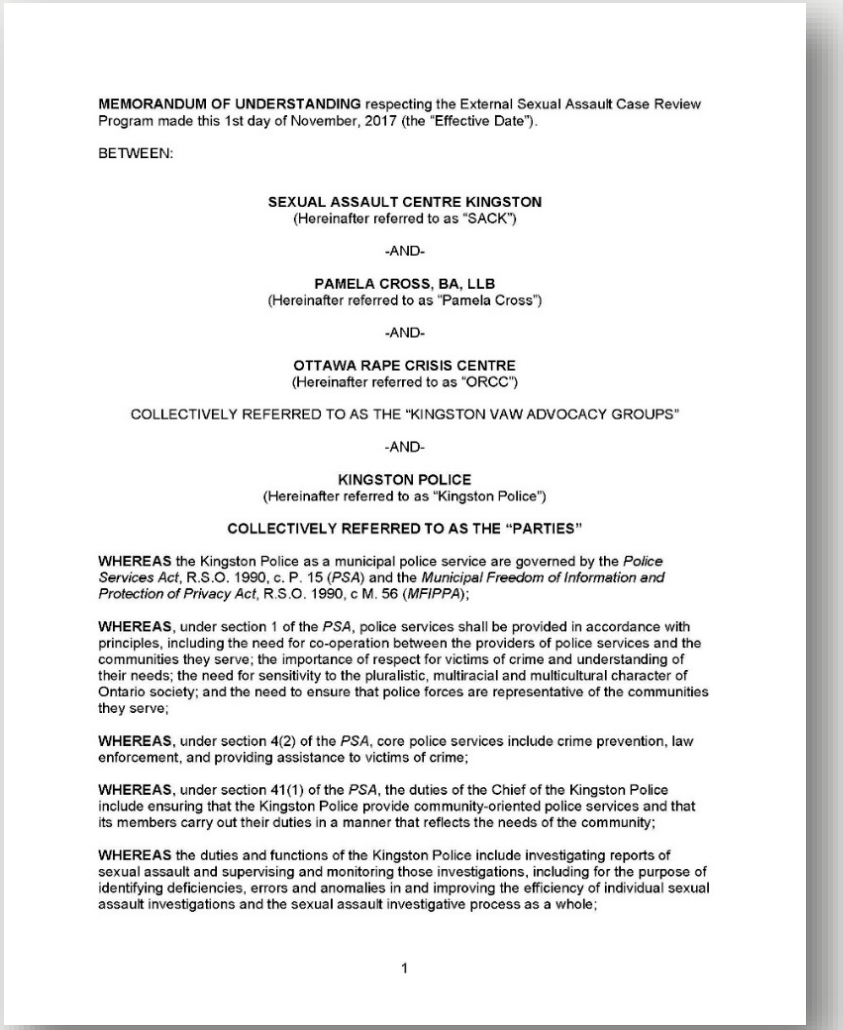
Cont'd

- 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;

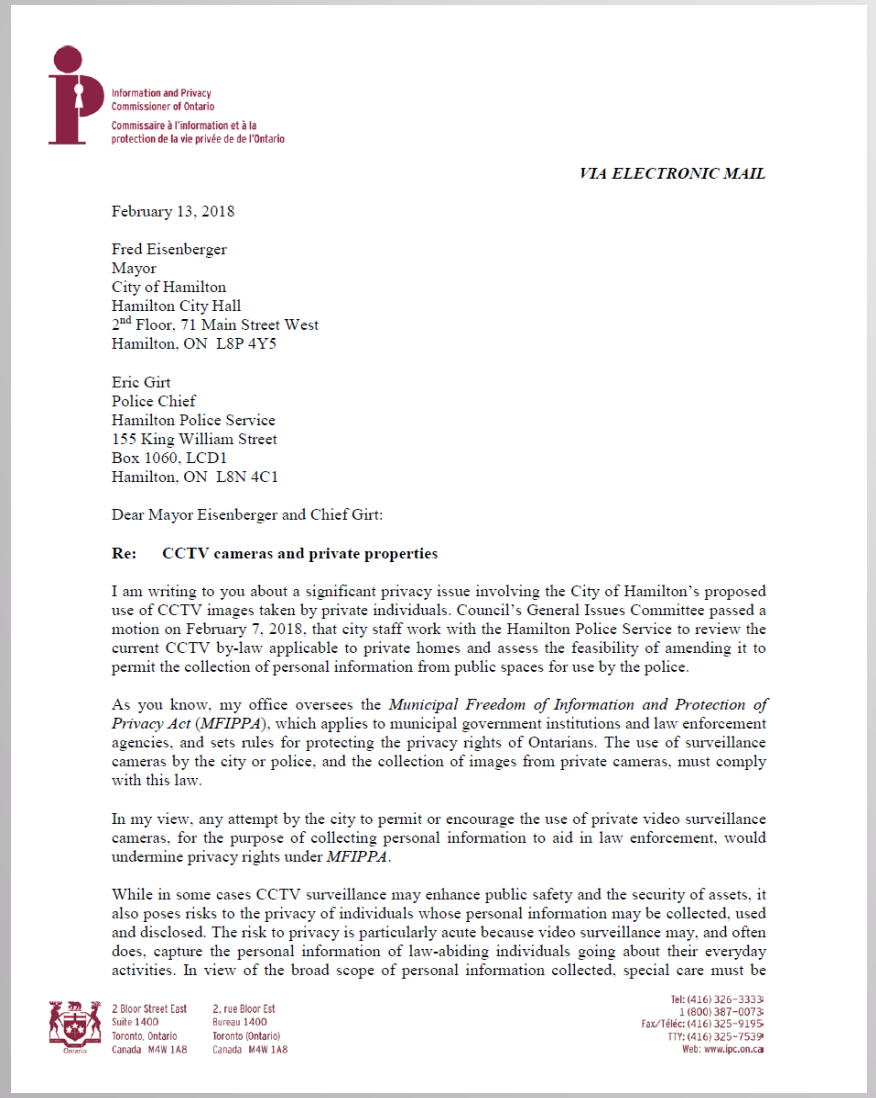
1

Surveillance Technologies

Surveillance Technologies

- IPC supports use of surveillance technologies to enhance community safety and deter unlawful activity, providing they are implemented in a manner that protects privacy
- Privacy implications associated with surveillance technologies include:
  - Potential to collect large amounts of personal information about individual users, including who they communicate with and what they communicate about
  - Ability to track the locations of individuals over time and to facilitate profiling of law-abiding individuals going about their everyday activities

City of Hamilton CCTV and Private Properties



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

VIA ELECTRONIC MAIL

February 13, 2018

Fred Eisenberger
Mayor
City of Hamilton
Hamilton City Hall
2nd Floor, 71 Main Street West
Hamilton, ON L8P 4Y5

Eric Girt
Police Chief
Hamilton Police Service
155 King William Street
Box 1060, LCD1
Hamilton, ON L8N 4C1

Dear Mayor Eisenberger and Chief Girt:

Re: CCTV cameras and private properties

I am writing to you about a significant privacy issue involving the City of Hamilton's proposed use of CCTV images taken by private individuals. Council's General Issues Committee passed a motion on February 7, 2018, that city staff work with the Hamilton Police Service to review the current CCTV by-law applicable to private homes and assess the feasibility of amending it to permit the collection of personal information from public spaces for use by the police.

As you know, my office oversees the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*), which applies to municipal government institutions and law enforcement agencies, and sets rules for protecting the privacy rights of Ontarians. The use of surveillance cameras by the city or police, and the collection of images from private cameras, must comply with this law.

In my view, any attempt by the city to permit or encourage the use of private video surveillance cameras, for the purpose of collecting personal information to aid in law enforcement, would undermine privacy rights under *MFIPPA*.

While in some cases CCTV surveillance may enhance public safety and the security of assets, it also poses risks to the privacy of individuals whose personal information may be collected, used and disclosed. The risk to privacy is particularly acute because video surveillance may, and often does, capture the personal information of law-abiding individuals going about their everyday activities. In view of the broad scope of personal information collected, special care must be

2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: (416) 326-3333
1 (800) 387-0073
Fax/Téléc: (416) 325-9195
TTY: (416) 325-7539
Web: www.ipc.on.ca

- 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
- Hamilton is encouraged to leave the by-law unamended

Sudbury's "Eye in the Sky"

- 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
- Our policy department worked with the police to make sure the details of the surveillance complied with privacy best practices

School Bus Cameras - Key Features

Features of school bus camera systems may include:

- Interior cameras
  - May record driver and students
- Exterior cameras (e.g., stop-arm cameras, dash cameras)
  - May record vehicles, pedestrians and driver
- Sound recording
  - May record driver and students
- Global Positioning System (GPS)
  - May record vehicle's location

Many capabilities are similar to video surveillance cameras

School Bus Cameras - What's Unique?

Cont'd

School bus camera systems present **different challenges** from traditional video surveillance systems:

- Mobile devices pose additional challenges that impact on privacy
- Notifying individuals who may be recorded can be challenging
- The amount of data captured and storage location may pose security related problems

School Bus Cameras - Best Practices

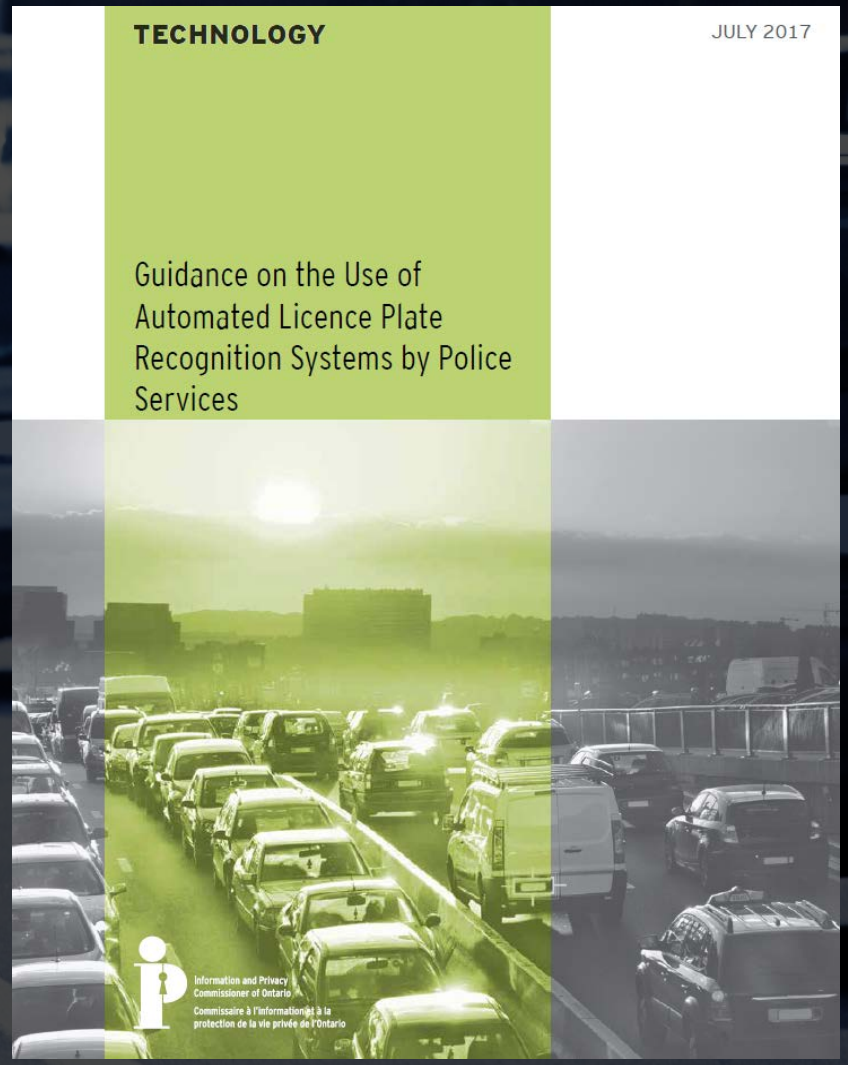
Cont'd

Best practices for school boards implementing a school bus camera program include:

- Consulting your school board's **Freedom of Information and Privacy Coordinator** and the **public**
- Conducting a **privacy impact assessment (PIA)**
- Establishing **policies** and **procedures**
- Establish a **privacy breach protocol**
- **Training** employees
- **Auditing** roles, responsibilities, and practices
- Consulting with **our office**

Automatic License-Plate Recognition (ALPR)

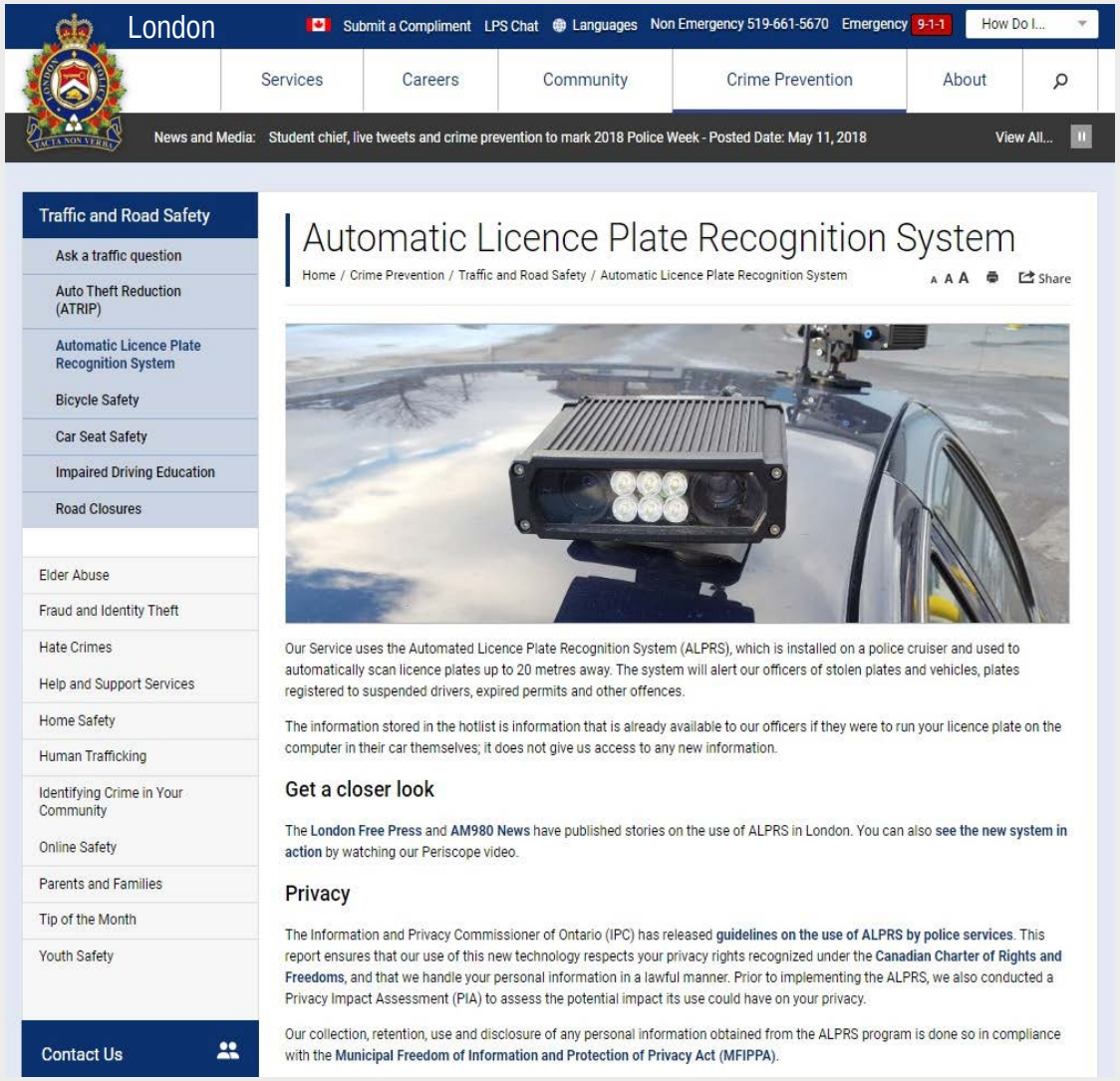
- ALPR systems used by police to match plates with a “hotlist” that may include stolen vehicles, expired plates and suspended drivers
- The IPC’s new guidance includes detailed advice on implementation, best practices for use in a privacy-protective manner
- Prepared in consultation with the OPP
- Implemented in 21 police services across Ontario



ALPR Best Practices

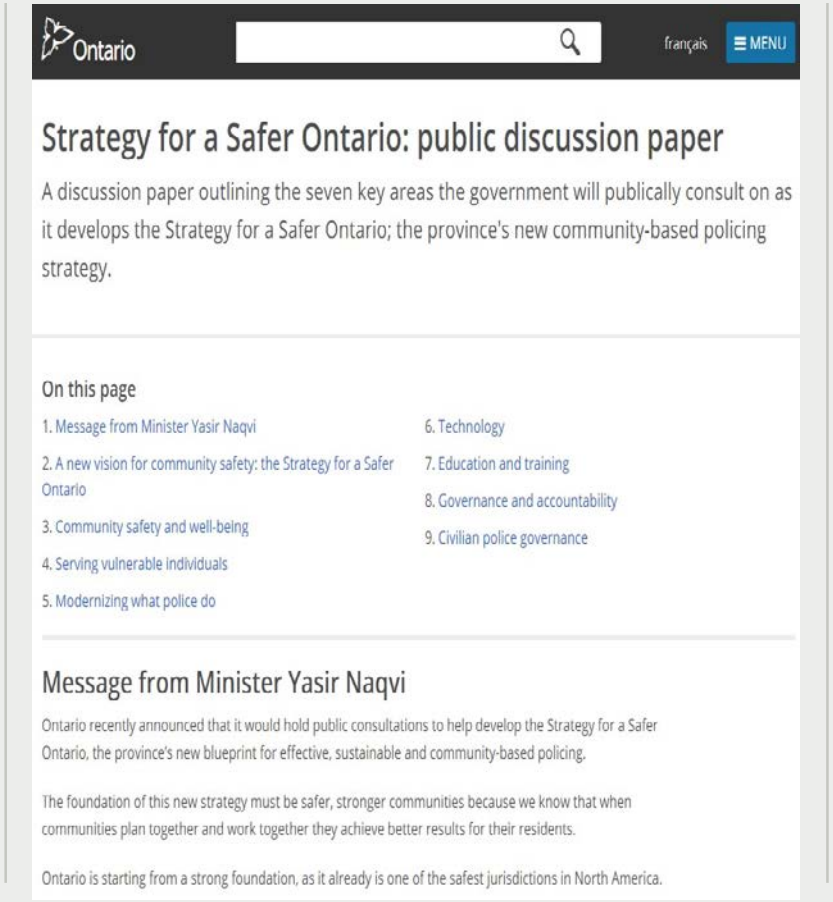
Cont'd

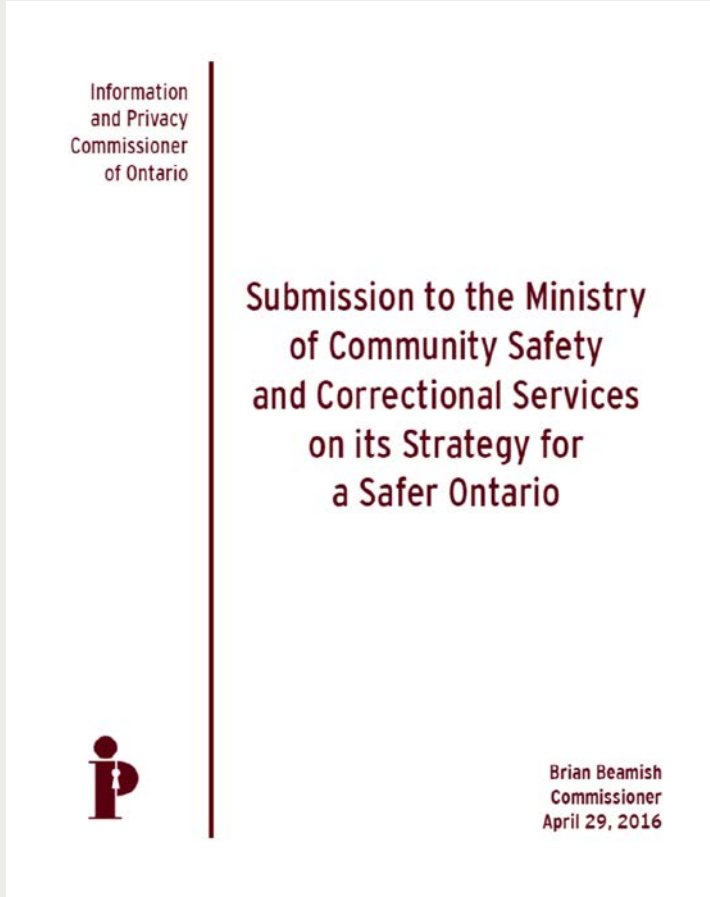
- Best practices include:
  - comprehensive **governance framework**
  - implementing **policies and procedures** to ensure the appropriate handling of personal information
  - **notice** to the public
  - **limiting retention** - non-hit data should be deleted as soon as practicable



Other Surveillance Technologies That Raise Privacy Concerns

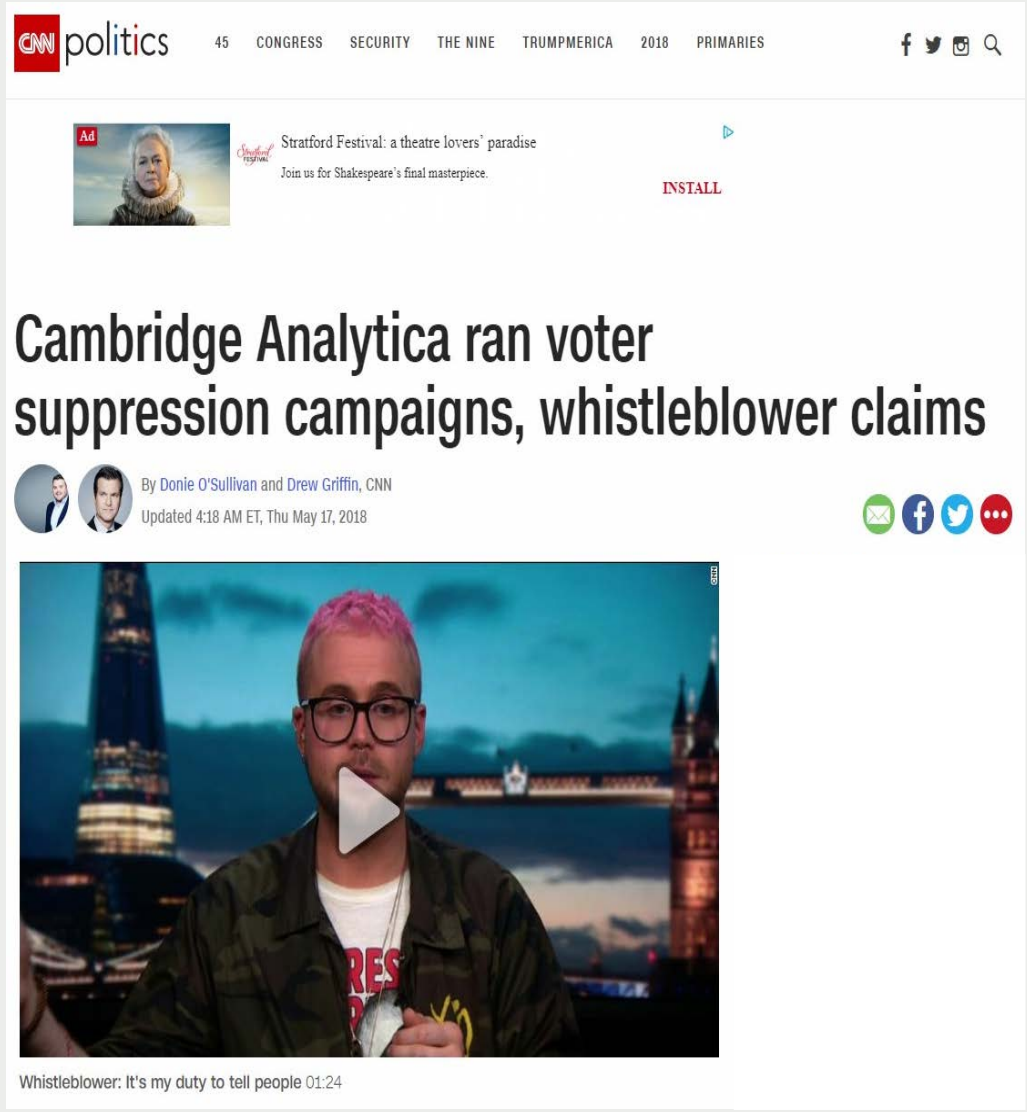
- Biometric Databases
- Facial Recognition
- Body-Worn Cameras
- IMSI Catchers
- Body Scanners
- Drones
- RFID
- Stingray Tracking Devices
- Smart Meters





Cambridge Analytica

- Collection of personal information of up to 87 million Facebook users, possibly more
- Data was allegedly used to influence voter opinion
- Raises questions about ethical standards for social media companies, political consulting organizations, and politicians
- Advocates have called for greater online protection for users, rights to privacy and restrictions on misinformation and propaganda



407 Privacy Breach

- Personal information for 60,000 customers was leaked through an internal theft
- Information included names, addresses and phone numbers but not financial information, licence plate numbers or customers' trip history
- Our office was contacted, as well as the police and the federal privacy commissioner

NATIONAL POST

Ontario PC candidate resigns after private 407 freeway confirms 'internal theft' of data on 60,000 customers

Samples of the leaked information suggest it was at one point in the hands of a company linked to an organizer who helped would-be PC candidates recruit members

The Highway 407 owners will offer free credit monitoring and identity-theft protection for a year to customers affected by the data leak. *Veronica Henri/Postmedia/File*

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

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

Cont'd

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

Cont'd

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

Cont'd

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)

Cont'd

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)
- 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
- 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

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 the *Police Services Act* to ensure that SIU 'no-charge' reports - reports that conclude that police will not face criminal charges in connection with the death or serious injury of a member of the public - are made public
  - Establishing police services data collection and retention systems to record human rights-based data on key interactions with civilians

New Police Accountability Legislation

Cont'd

- June 30, 2018 – the Special Investigations Unit will be renamed the Ontario Special Investigations Unit (OSIU) and must ***publish 'no-charge' reports***
- January 1, 2019 – the Ministry of Community Safety and Correctional Services (MCSCS) will be able to collect personal information from police services
- January 1, 2020 – the Ontario Policing Complaints Agency (OPCA) will be authorized to collect personal information specified by regulation
- The IPC will oversee OSIU, MCSCS and OPCA compliance with privacy legislation

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 record check providers can tell prospective employers, volunteer agencies and others about Ontarians
- Prohibits the release of street checks and mental health records and the restricts release of non-conviction records in police record checks
- Leading edge legislation that addresses public safety while protecting privacy

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

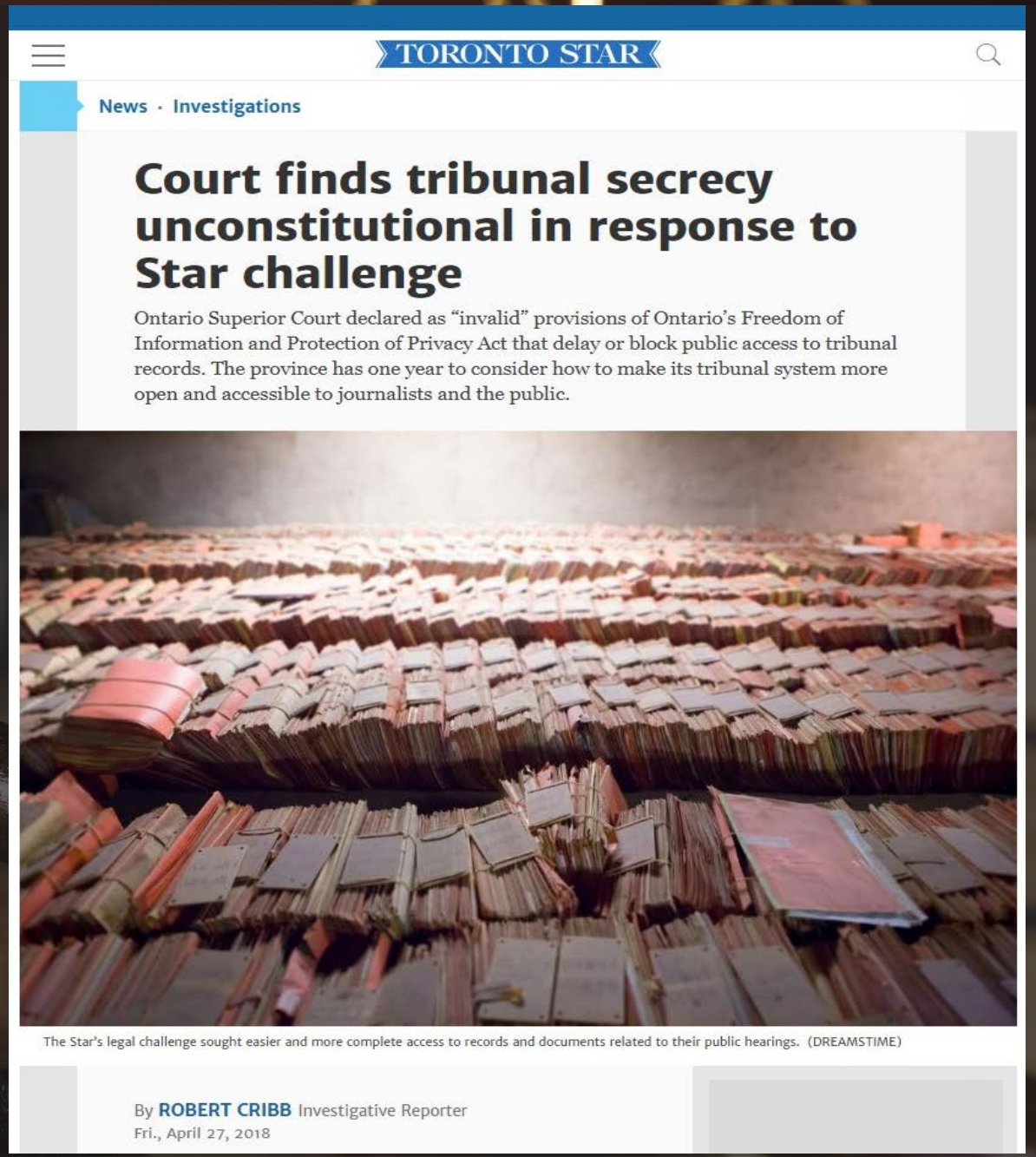
Health minister flags 500 doctors who made more than $1 million last year in a bid for public support in reforming outdated OHIP system.

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



TORONTO STAR

News · Investigations

Court finds tribunal secrecy unconstitutional in response to Star challenge

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 Star's legal challenge sought easier and more complete access to records and documents related to their public hearings. (DREAMSTIME)

By **ROBERT CRIBB** Investigative Reporter
Fri., April 27, 2018

Resources

IPC Fact Sheets

- Published in response to frequently asked questions about access, privacy and technology
- Recently released:
  - Fees, Fee Estimates and Fee Waivers
  - Disposing of Your Electronic Media
  - Reasonable Search

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
0:06 / 12:51
CC
HD
YouTube

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