Privacy in our Smart Cities

Renee Barrette, Director of Policy

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

ITS • STI
CANADA
2018
ANNUAL CONFERENCE
& GENERAL MEETING

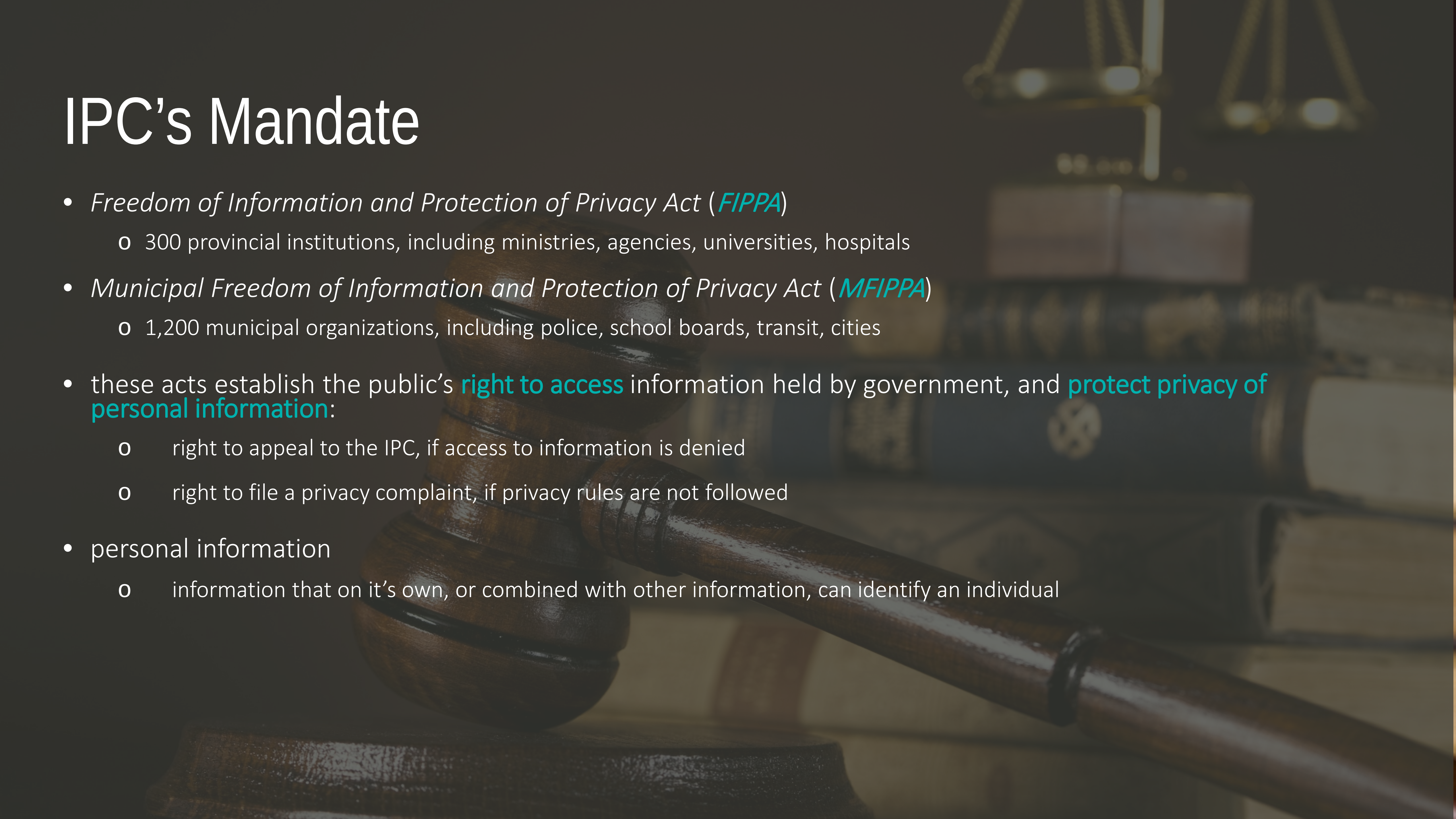
Agenda

- Role of Ontario’s Information and Privacy Commissioner
- What is a smart city
- Privacy risks
- Mitigating controls
- Open data
- IPC engagement

Our Office

- Commissioner appointed by, reports to, Legislative Assembly to ensure impartiality
- independent review of government decisions and practices on access and privacy
- oversees compliance with three access and privacy laws

IPC’s Mandate



- *Freedom of Information and Protection of Privacy Act* (*FIPPA*)
  - 300 provincial institutions, including ministries, agencies, universities, hospitals
- *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)
  - 1,200 municipal organizations, including police, school boards, transit, cities
- these acts establish the public’s right to access information held by government, and protect privacy of personal information:
  - right to appeal to the IPC, if access to information is denied
  - right to file a privacy complaint, if privacy rules are not followed
- personal information
  - information that on it’s own, or combined with other information, can identify an individual

Privacy in the Private Sector

- private sector privacy law, *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) overseen by Privacy Commissioner of Canada
  - Ontario does not have its own private sector privacy law
  - *PIPEDA* applies to businesses in Ontario and throughout Canada (except BC, AB, QC) including banks, airlines, retail stores

Smart Cities

- smart cities are communities that use connected technologies to collect and analyze data to improve services for citizens

- information collected, used, disclosed by smart cities can, often does, include personal information

- depending on the technology and how it’s implemented, different privacy laws may apply

M/FIPPA Requirements

- Ontario’s public sector privacy and access laws create a privacy protection scheme which institutions and their agents must follow, including:
  - limits on the collection, use and disclosure of personal information
  - requirements for notice of collection
  - standards for security, retention, and secure disposal
  - oversight mechanism - privacy complaints, investigations, orders, recommendations, public reporting

Smart city examples

- LED streetlights with smart sensors
  - sensors that dim streetlights when no one is around
  - potential for video and audio (CCTV) attachments
- smart traffic lights
- real-time parking apps that map out nearest available spots

Privacy risks

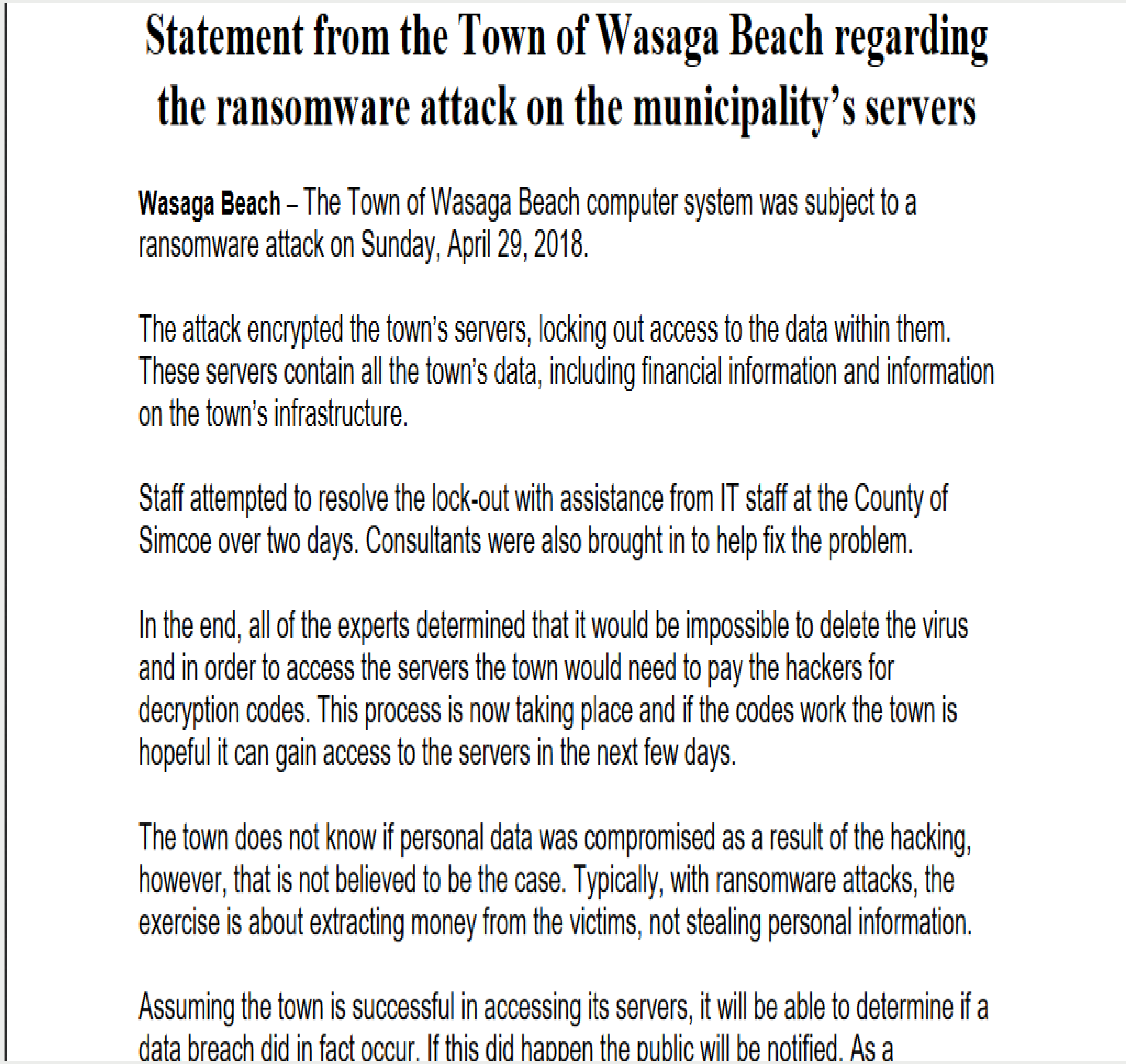
Privacy risks

- privacy is not a barrier to smart cities, but they require robust privacy protections
- without safeguards in place, large amount of sensitive personal information may be collected, used, disclosed without lawful authority
- this information could be:
  - used to track people as they go about their daily activities
  - used and disclosed for purpose that is inconsistent with the original purpose, without consent
  - subject to security breaches, including cyberattacks

Privacy risks - examples

Ransomware

- computers may be infected by
  - phishing attacks
  - software exploits
- protect your organization by
  - employee training
  - limiting user privileges
  - software protections and backups
- breach response procedures
- IPC Fact Sheet Protecting Against Ransomware



Statement from the Town of Wasaga Beach regarding the ransomware attack on the municipality's servers

Wasaga Beach – The Town of Wasaga Beach computer system was subject to a ransomware attack on Sunday, April 29, 2018.

The attack encrypted the town's servers, locking out access to the data within them. These servers contain all the town's data, including financial information and information on the town's infrastructure.

Staff attempted to resolve the lock-out with assistance from IT staff at the County of Simcoe over two days. Consultants were also brought in to help fix the problem.

In the end, all of the experts determined that it would be impossible to delete the virus and in order to access the servers the town would need to pay the hackers for decryption codes. This process is now taking place and if the codes work the town is hopeful it can gain access to the servers in the next few days.

The town does not know if personal data was compromised as a result of the hacking, however, that is not believed to be the case. Typically, with ransomware attacks, the exercise is about extracting money from the victims, not stealing personal information.

Assuming the town is successful in accessing its servers, it will be able to determine if a data breach did in fact occur. If this did happen the public will be notified. As a

Public trust and confidence

- 9 in 10 Canadians are concerned about privacy
  - (Privacy Commissioner of Canada, 2015)

- important in a free and democratic society - individuals may censor their activities when being watched

- protection of personal information is fundamental to maintaining the public's trust and confidence

Privacy protections and controls

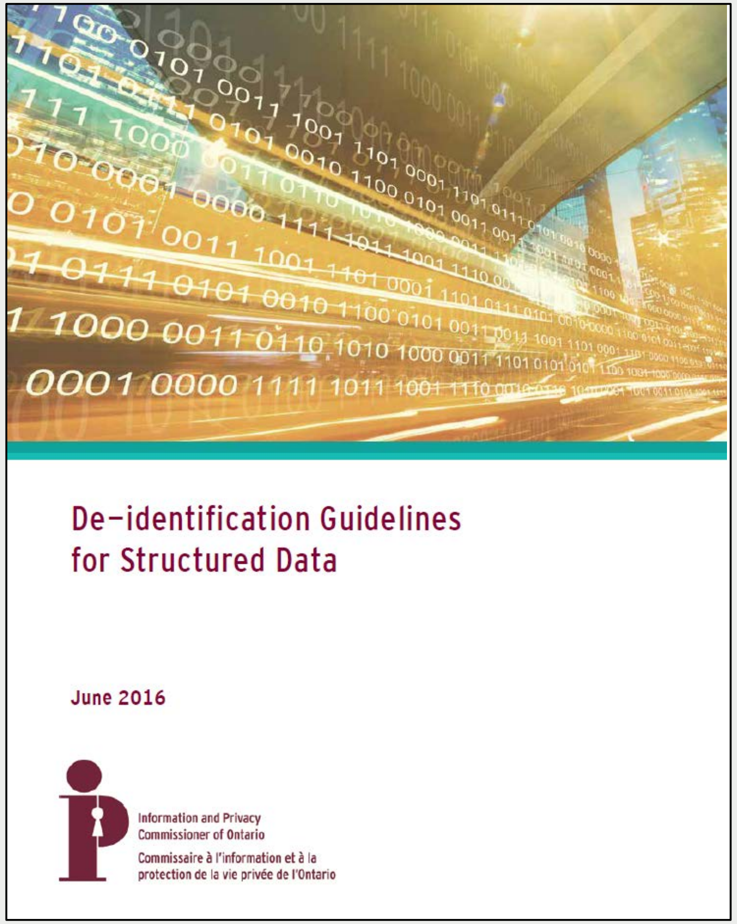
Privacy protections and controls

- data minimization
  - avoid ‘tech for tech’s sake’
  - define the problem and consider less privacy invasive alternatives
  - do you need to collect personal information

- de-identification
  - removing personal information from a record or data set
  - de-identify at earliest opportunity
  - guard against re-identification

Privacy protections and controls continued…

- de-identification guidelines
- introduce basic concepts and techniques of de-identification and provides a step-by-step protocol for de-identifying structured data
- discuss key issues of:
  - direct and indirect identifiers
  - public, non-public and semi-public release models
  - different re-identification attacks
  - measuring and calculating re-identification risks
  - common de-identification techniques
- won 2017 ICDPPC Award for “Excellence in Research”



De–identification Guidelines
for Structured Data

June 2016

Information and Privacy
Commissioner of Ontario

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

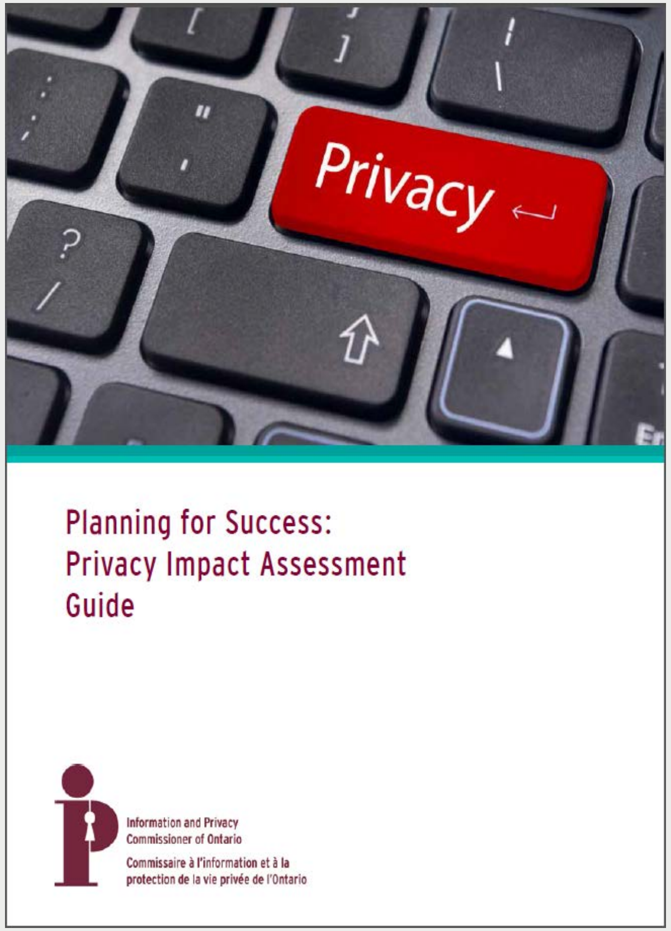
Privacy protections and controls continued…

- consent
  - where required by law
  - opportunity to opt out, where feasible
- notice, community engagement and project transparency
- reasonable measures to secure personal information
- data governance and privacy management program
  - policies that address privacy and security requirements
  - contractual protections and accountability

and …

Privacy protections and controls continued…

- Threat Risk Assessment
  - process designed to identify security risks associated with information systems and technology
- Privacy Impact Assessment
  - **guidance**: tool to identify privacy effects, mitigate risks, of a given project
  - simplified 4-step methodology with tools



Planning for Success:
Privacy Impact Assessment
Guide

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

Open Data

- information collected or created should be considered a public resource
- to support local innovation, address community needs, data collected/created should be made available to the public as open data, while ensuring that personal information is de-identified

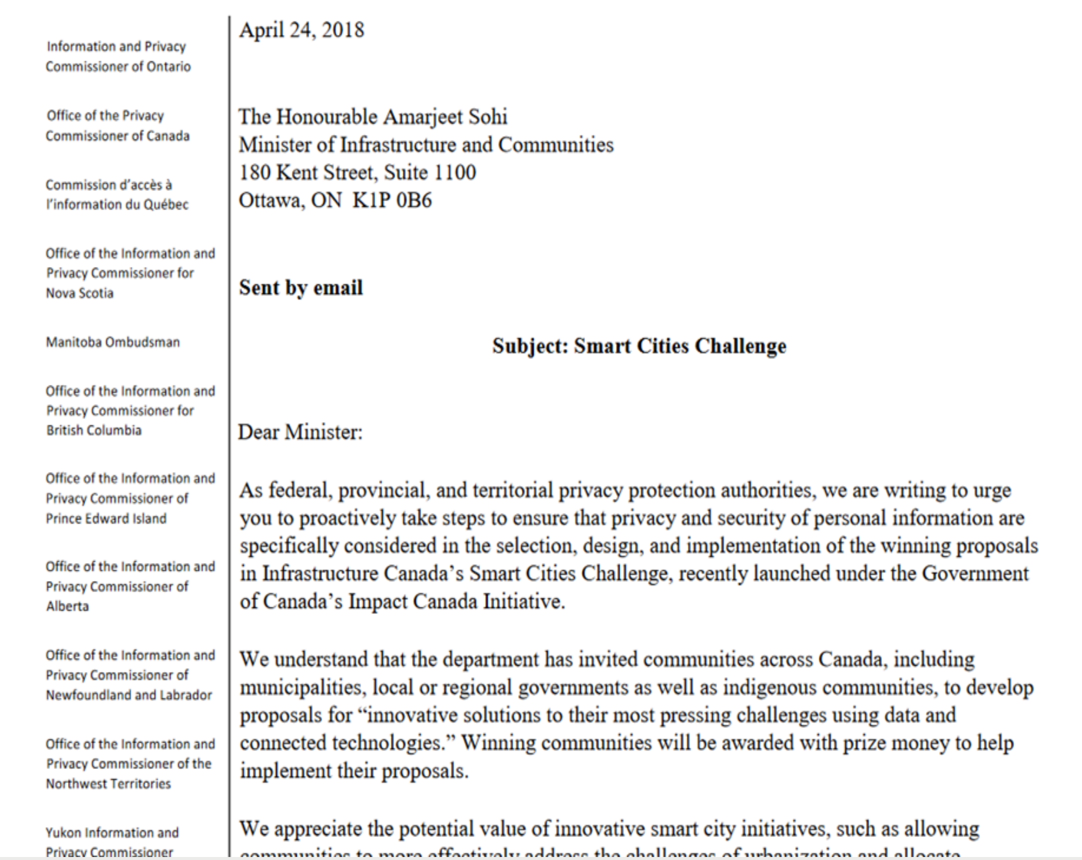
Engagement on Smart Cities

IPC’s policy role

- conduct 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, public speaking
- develop guidance to help organizations understand their legislative obligations, and help the public understand their access and privacy rights

Canada’s Smart Cities Challenge

- challenge invites communities to compete for funding for smart city projects
- IPC led an open letter initiative with privacy authorities across Canada, urging federal government to ensure strong privacy protections are included as selection criteria
- three finalist communities from Ontario received $250,000 to develop their final proposal



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

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

Sidewalk Toronto

- Sidewalk Labs, Waterfront Toronto have agreed to develop a plan for a new smart city development
  - "Sidewalk Toronto" would represent North America's largest smart city project
- we are engaged with both players and will continue to do so
- Sidewalk Toronto's Responsible Data Use Framework includes commitment to build on the recommendations cited in our Smart Cities Challenge letter

Guidance

- fact sheet for the public
  - defines smart cities
  - provides examples
  - identifies risks
  - outlines individual's rights under Ontario's privacy laws, including right to access their own information

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

IPC’s open door policy

- achieving the kind of balance we are striving for is not possible without involvement of other agencies and stakeholders
- IPC has an open door policy for any Ontario institution considering programs which may impact privacy
- vast majority of privacy challenges can be addressed through collaboration
- key is to address privacy concerns from the outset

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