Smart Cities: Building in Privacy and Ensuring Public Trust

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

SMART CITY & IoT EXPO

October 9, 2018

Our Office

- Provides independent review of government decisions and practices on access and privacy
- Commissioner is appointed by, and reports to, the Legislative Assembly to ensure impartiality
- Oversees Ontario's access and privacy laws
- These laws establish the public's right to access government-held information and protect their personal privacy rights

IPC's Legislation

- *Freedom of Information and Protection of Privacy Act* (*FIPPA*)
  - 300 provincial institutions including ministries, agencies, boards, universities
- *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)
  - 1,200 municipal organizations, including police, school boards, transit, cities
- *Personal Health Information Protection Act* (*PHIPA*)
  - those involved in delivery of health care including hospitals, pharmacies, laboratories, doctors, dentists and nurses

Private Sector Legislation

- *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)
- overseen by the Privacy Commissioner of Canada
- *PIPEDA* applies to businesses in Ontario and throughout Canada (except BC, AB, QC)

Smart Cities

The Big Data Shift

- Data as a tool for shaping and improving policies, programs and services
- Supported by advancements in computing and technology:
  - new sources of personal information
  - unlimited capacity to store data
  - better techniques to link records and data
  - algorithms that can make predictions based on data
- Using data this way raises a number of privacy, fairness and ethical concerns

Information Collection

- Information collected, used, and disclosed by smart cities can, and often does, include personal information
- May be collected by municipalities, contractors, or private companies:
  - energy consumption patterns
  - video and audio recordings
  - vehicle licence plate numbers
  - mobile device and other identifiers

What Privacy Laws Apply?

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

- data collected by or on behalf of a municipality; no collection of personal information unless:
  - authorized by statute
  - used for law enforcement, or
  - when necessary for a lawfully authorized activity

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

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 information for other purposes without consent (scope creep)
- security breaches (cyberattacks)

How is data being collected?

How is it being used?

The Guardian

'Living laboratories': the Dutch cities amassing data on oblivious residents

In Eindhoven and Utrecht smart tech is tackling traffic, noise and crime. But with privacy laws proving futile and commercial companies in on the act, are the plans as benign as they seem?

Using a smartphone in Utrecht, where €80m has been invested in data-driven management. Photograph: Alamy

Cyberattacks

Systems infected by:

- phishing schemes to gain access to passwords/information
- ransomware and other software exploits used to gain control of computer systems

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
These servers contain all the town's data, including
on the town's infrastructure

Ontario police warn of recent cyberattacks targeting local governments

THE CANADIAN PRESS Updated: September 14, 2018

Privacy Protections

Privacy Protections

Data minimization

- avoid ‘tech for tech’s sake’
- define goals or objectives at the outset
- consider less privacy invasive ways to achieve them

De-identification

- remove personal information to protect the privacy of individuals
- guard against re-identification of data

Privacy Protections and Controls

Data governance and privacy management program:

- policies to address privacy and security requirements
- contractual protections and accountability are key in public-private partnerships

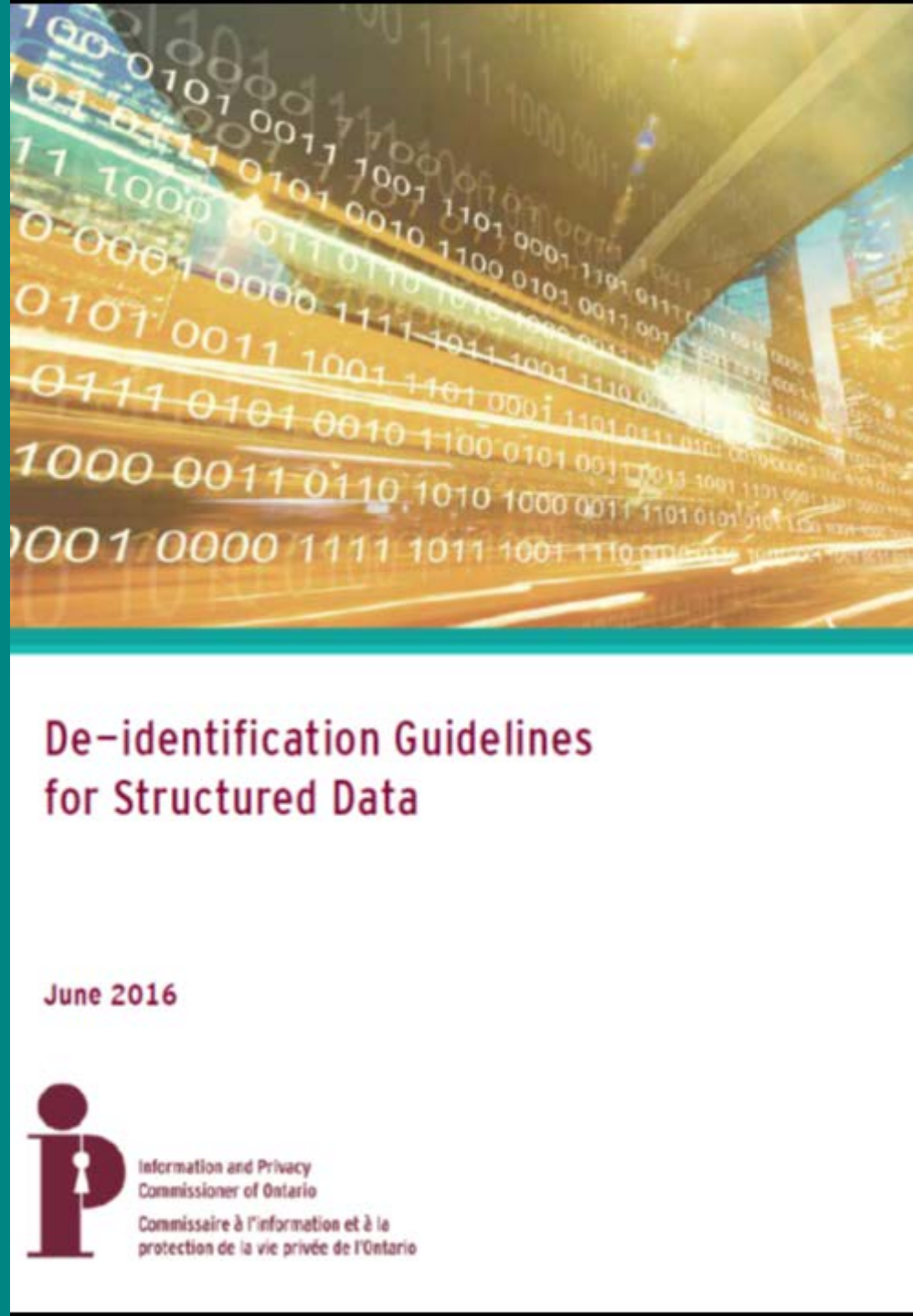
Consent:

- where required by law
- opportunity to opt out where feasible

Community engagement and project transparency

De-identification Guidelines

- Outlines basic de-identification concepts and techniques as well as a step-by-step protocol
- Discussion of:
  - common de-identification methods
  - data release models
  - types of re-identification attacks
  - calculating re-identification risks
- Winner of the 2017 ICDPPC Award for Excellence in Research



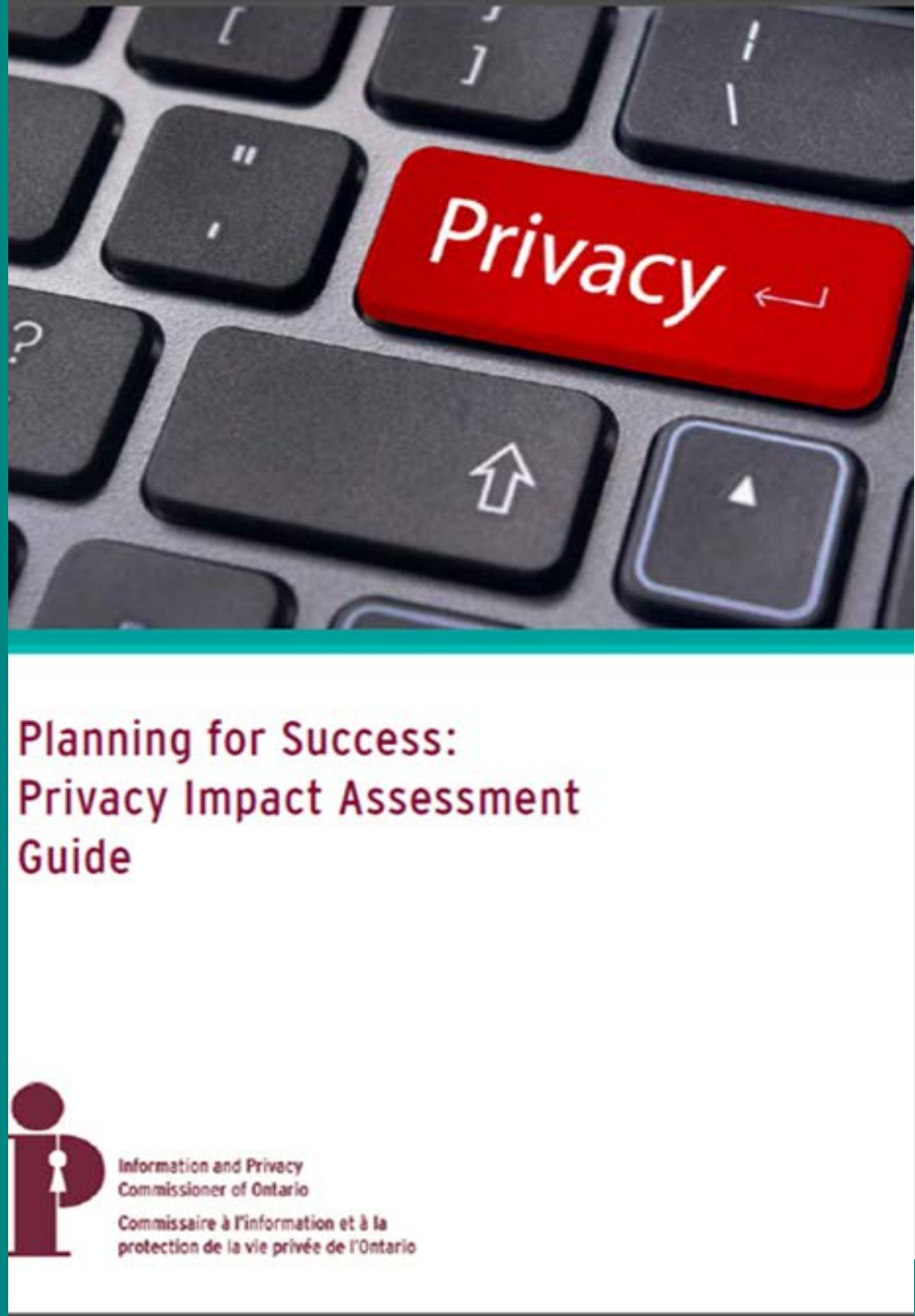
Assess Privacy Risks

Privacy Impact Assessment

- process to identify and assess the potential privacy risks of a project or program
- can eliminate or reduce risks to an acceptable level

Threat Risk Assessment

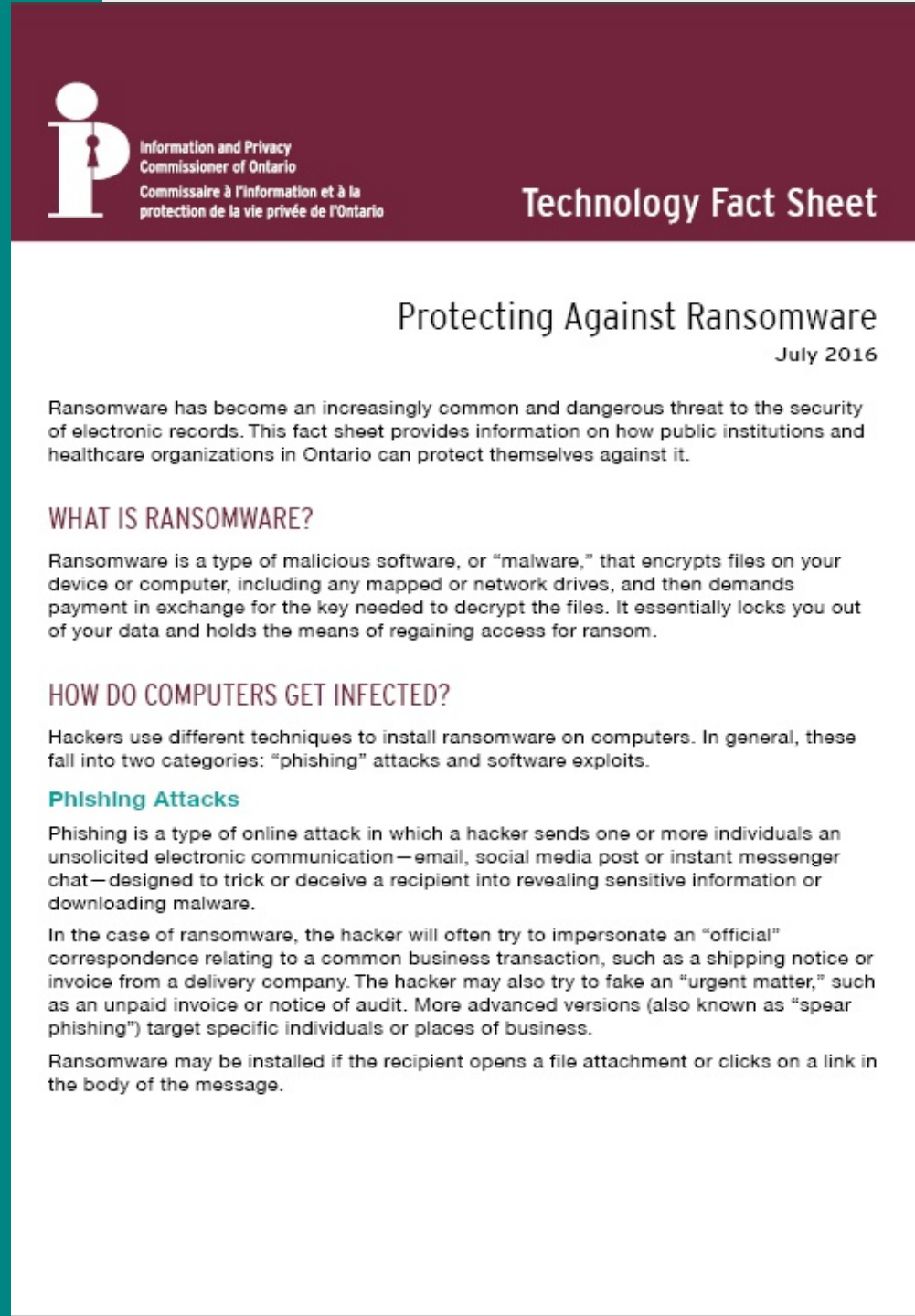
- used to identify security risks associated with information systems and technology



Guard Against Ransomware

Protect your organization

- train employees
- limit user privileges
- use software protections and back-ups
- have an incident response plan in place



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.

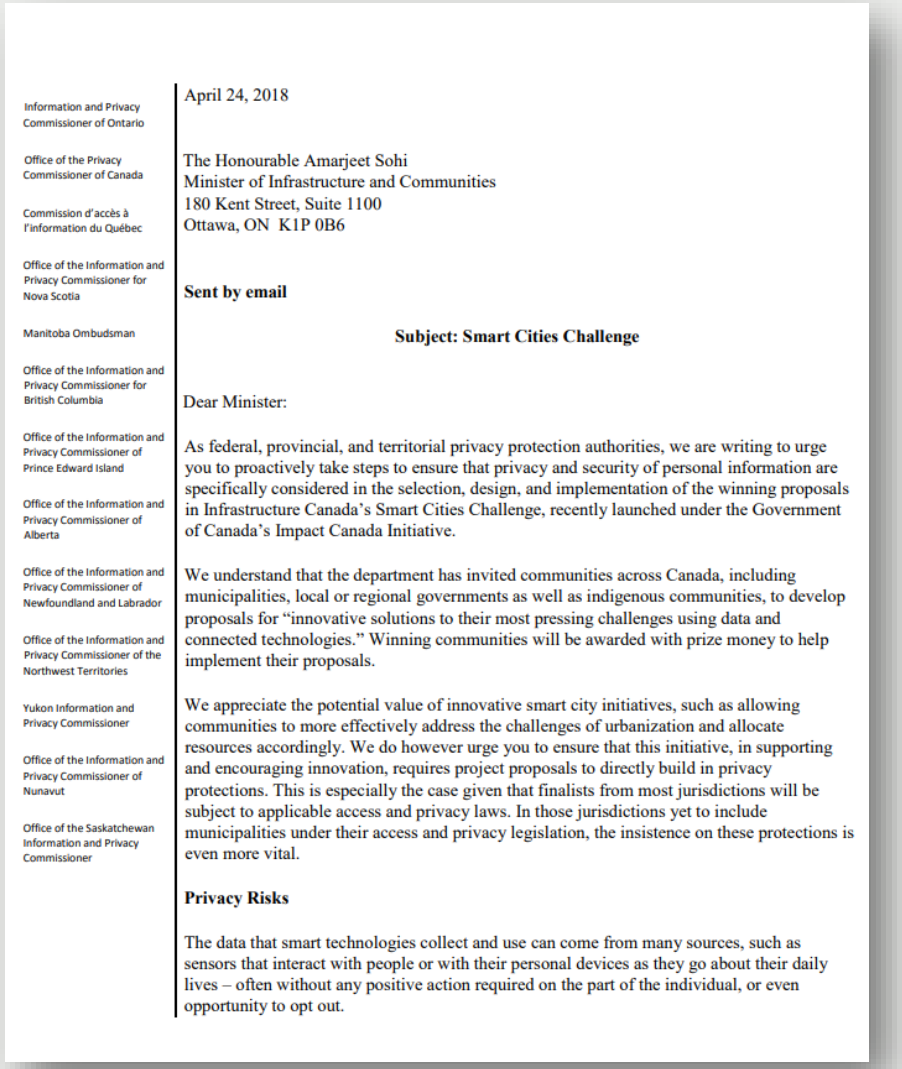
Open Data

- Information collected or created should be considered a public resource
- Made available as de-identified open data to support local innovation and address community needs

Engagement on Smart Cities

Canada's Smart Cities Challenge

- Strong **privacy protections** must be **built into** smart city projects from the start
- The message of cross-Canada privacy authorities to minister in charge of Canada's Smart Cities Challenge
- As a result finalists are required to consult with the privacy authority in their jurisdiction and complete a privacy impact assessment
- Three finalist communities from Ontario:
  - Biigtigong Nishnaabeg (Pic River First Nation)
  - City of Guelph and Wellington County
  - Region of Waterloo



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.

Sidewalk Toronto

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

Public Education

The facts about smart cities

- What they are
- How they can affect privacy rights
- How to minimize privacy risks

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

"A democratic society relies upon the participation of an informed citizenry. A city cannot be truly innovative and respect the rights of its residents if only a sliver of public officials have the power to speak for — or to ignore — the broader community. Every resident has the right to participate in decision-making processes that impact their constitutional rights."

— American Civil Liberties Union

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