SMART CITIES

BUILDING IN PRIVACY AND ENSURING PUBLIC TRUST

4th Annual Intelligent Cities Summit – October 8, 2019

David Goodis, Assistant Commissioner
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

Agenda

- Ontario's Information and Privacy Commissioner
- Benefits of smart city technologies
- Privacy risks
- Mitigating controls
- 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

Ontario's Legislative Framework

Public Sector	Health Sector	Private Sector
Government provincial ministries, agencies, hospitals, universities, cities, police, schools, hydro *Freedom of Information and Protection of Privacy Act* (*FIPPA*) *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)	**Health care providers** hospitals, pharmacies, labs, doctors, dentists, nurses *Personal Health Information Protection Act* (*PHIPA*)	**Private businesses** *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)
IPC/O oversight	IPC/O oversight	Privacy Commissioner of Canada oversight

Smart Cities

The Big Data Shift

- data used to shape, improve policies, programs, services

- supercharged 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

What can smart cities offer?

Improved quality of life

- less congestion and traffic accidents
- safety for cyclists and pedestrians
- cleaner environment
- efficient use of public resources
- better informed citizens

Information Collection

- information collected, used, disclosed by smart city technologies often includes **personal information**

- may be collected by municipalities, private companies or both! (public-private partnerships)
  - energy consumption patterns
  - video and audio recordings
  - vehicle licence plate numbers
  - mobile device ID, other identifiers

Privacy risks

Privacy Risks

- privacy is not a barrier to smart cities, but they require robust privacy protections

- without safeguards in place, unreasonably large amounts of personal information may be collected, used, disclosed

- potential hazards:
  - tracking individuals as they go about their daily activities (surveillance)
  - using and disclosing information for other purposes without consent (function creep)

What data is being collected?

In what way?

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 and controls

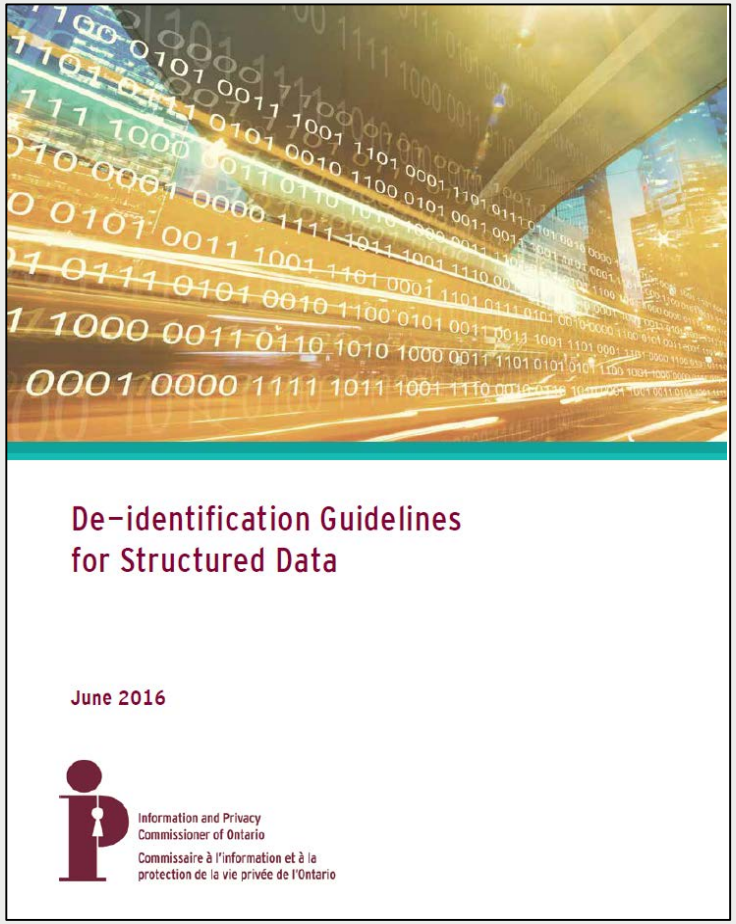
Privacy protections and controls

- 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

- de-identification guidelines
- basic concepts and techniques of de-identification
- step-by-step to de-identify structured data
- key elements
  - direct and indirect identifiers
  - public, non-public, semi-public release
  - re-identification risks
- won 2017 ICDPPC Award for “Excellence in Research”



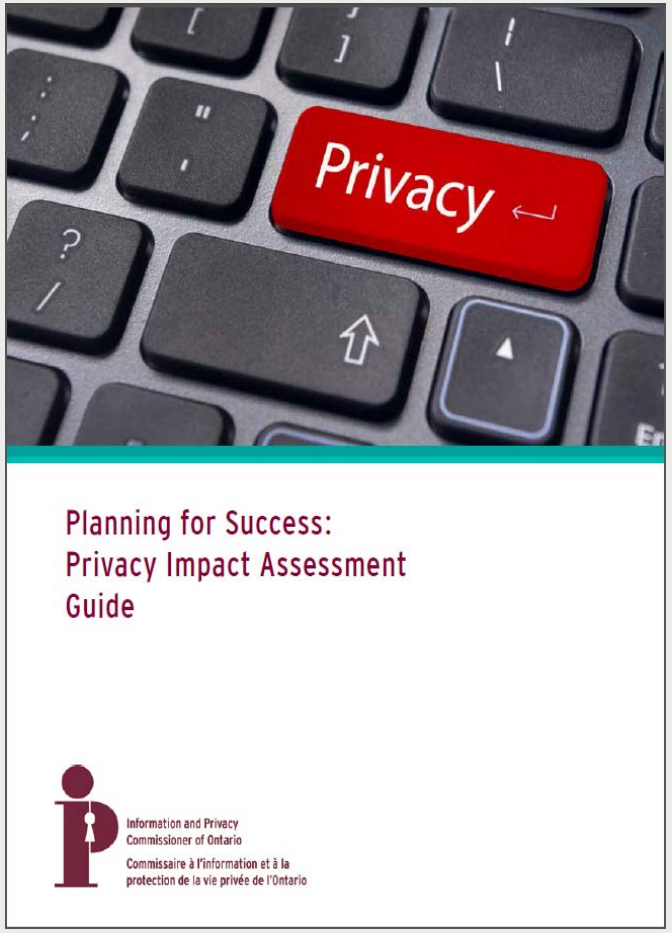
Privacy protections and controls

- notice, community engagement, 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

Privacy protections and controls

- Threat Risk Assessment
  - process designed to identify security risks associated with information systems and technology

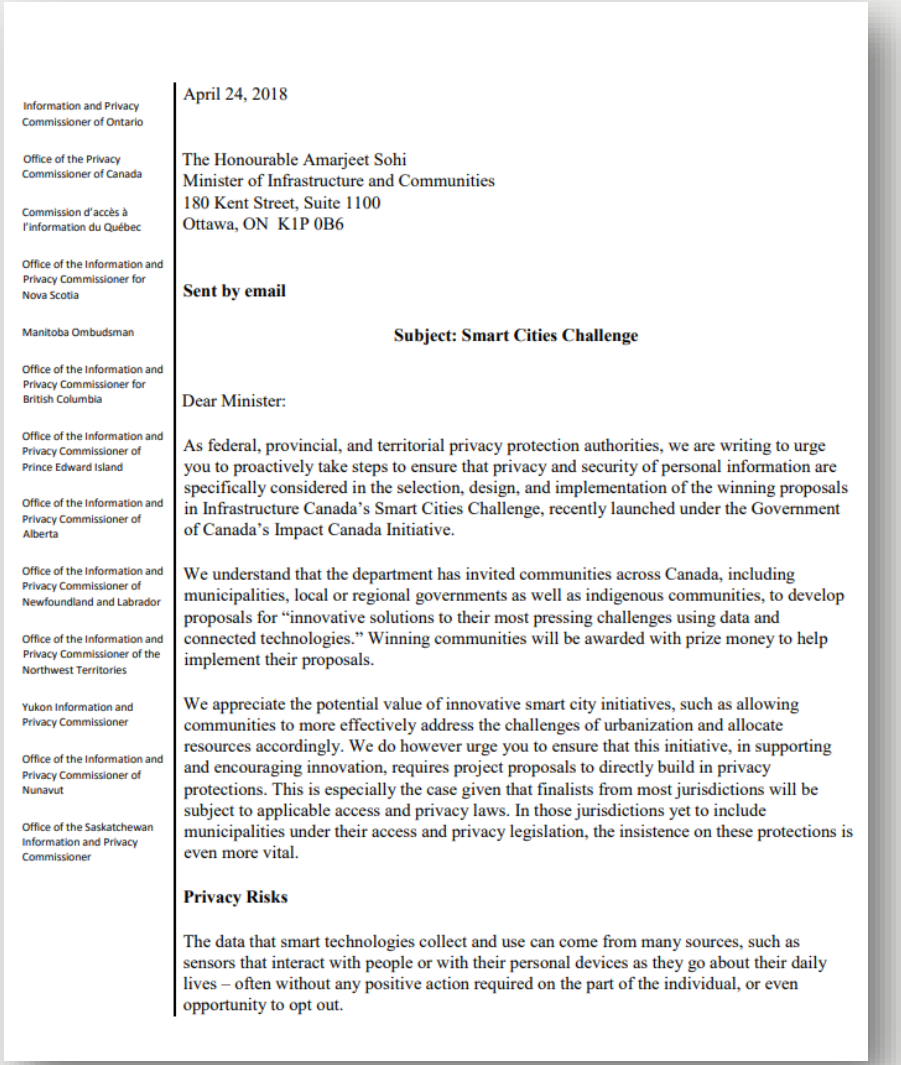
- Privacy Impact Assessment
  - tool to identify privacy effects, mitigate risks, of a given project
  - simplified 4-step methodology with tools



Engagement on Smart Cities

Canada's Smart Cities Challenge

- strong privacy protections must be built into smart city projects from the start
- cross-Canada privacy authorities message to minister in charge of Canada's Smart Cities Challenge
- finalists now must consult with privacy authority in their jurisdiction, complete privacy impact assessment
- four Ontario finalists:
  - Biigtigong Nishnaabeg (Pic River First Nation)
  - City of Guelph/Wellington County (winner)
  - Mohawk Council of Akwesasne
  - 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 Labs' Quayside proposal

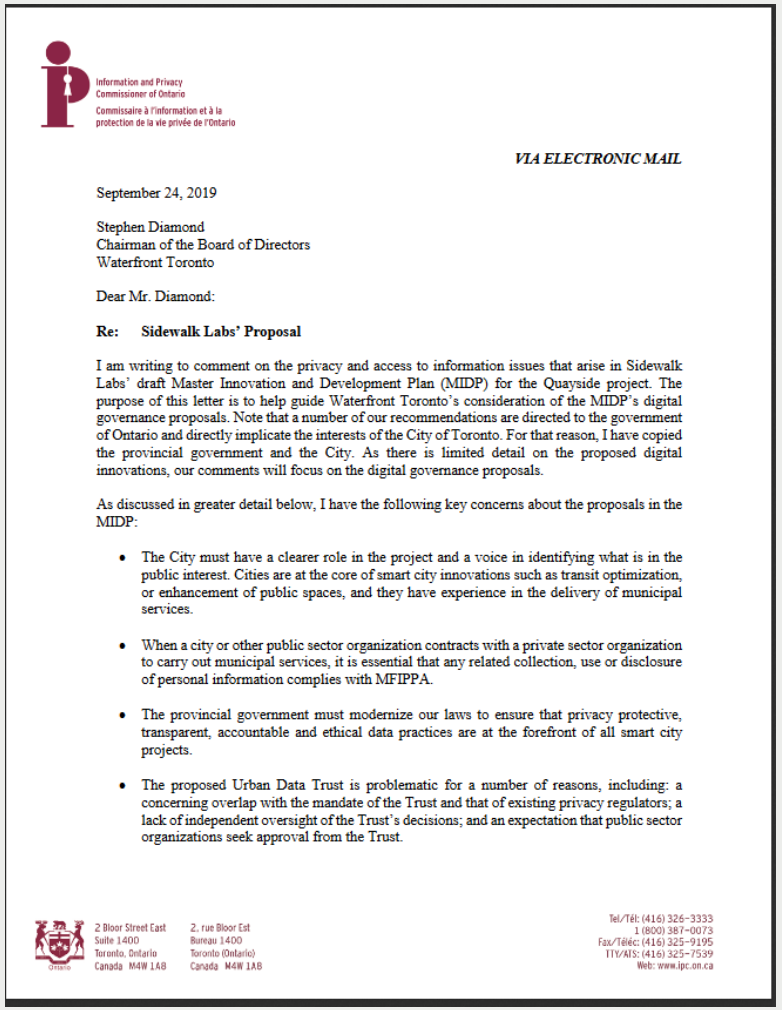
- Sidewalk Labs/Waterfront Toronto exploring project to revitalize 12-acre parcel

- Sidewalk Labs' digital governance proposal includes call for independent urban data trust to manage data collected at Quayside

Quayside

IPC comments on privacy issues arising from Sidewalk Labs' draft plan

- clearer role for City/MFIPPA critically important
- Urban Data Trust – who oversees them? How do they manage overlapping jurisdiction? Does it makes sense for public sector to seek their approval?
- provincial government must modernize our laws to ensure privacy, transparency, accountability, ethical data practices in smart city projects



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

VIA ELECTRONIC MAIL

September 24, 2019

Stephen Diamond
Chairman of the Board of Directors
Waterfront Toronto

Dear Mr. Diamond:

Re: Sidewalk Labs' Proposal

I am writing to comment on the privacy and access to information issues that arise in Sidewalk Labs' draft Master Innovation and Development Plan (MIDP) for the Quayside project. The purpose of this letter is to help guide Waterfront Toronto's consideration of the MIDP's digital governance proposals. Note that a number of our recommendations are directed to the government of Ontario and directly implicate the interests of the City of Toronto. For that reason, I have copied the provincial government and the City. As there is limited detail on the proposed digital innovations, our comments will focus on the digital governance proposals.

As discussed in greater detail below, I have the following key concerns about the proposals in the MIDP:

- The City must have a clearer role in the project and a voice in identifying what is in the public interest. Cities are at the core of smart city innovations such as transit optimization, or enhancement of public spaces, and they have experience in the delivery of municipal services.
- When a city or other public sector organization contracts with a private sector organization to carry out municipal services, it is essential that any related collection, use or disclosure of personal information complies with MFIPPA.
- The provincial government must modernize our laws to ensure that privacy protective, transparent, accountable and ethical data practices are at the forefront of all smart city projects.
- The proposed Urban Data Trust is problematic for a number of reasons, including: a concerning overlap with the mandate of the Trust and that of existing privacy regulators; a lack of independent oversight of the Trust's decisions; and an expectation that public sector organizations seek approval from the Trust.

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

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

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

Public Education

The facts about smart cities

- What are they?
- How can they affect privacy?
- How do we 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

IPC's open door policy

- achieving balance not possible without involving other agencies and stakeholders
- IPC has 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