



Information Collection

- Information collected, used, and disclosed by smart city technologies can, and often does, include personal information
- May be collected by municipalities, private companies or as part of public-private partnerships
 - energy consumption patterns
 - video and audio recordings
 - vehicle licence plate numbers
 - mobile device and other identifiers

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 and disclosing information for other purposes without consent (function creep)
- security breaches (cyberattacks)

Which Privacy Laws Apply?

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

- No **collection** of personal information unless:
 - authorized by statute
 - used for law enforcement
 - when necessary for a lawfully authorized activity
- No use or disclosure unless for the same, or a consistent, purpose

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

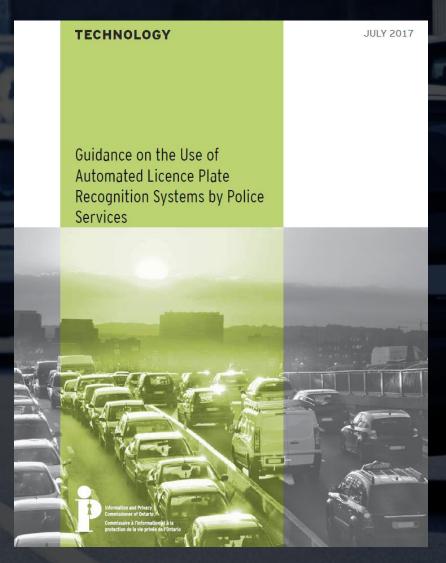


Automatic License-Plate Recognition (ALPR)

Best practices for implementing an ALPR program include:

- conducting a Privacy Impact Assessment
- ensuring a comprehensive governance framework
- deleting non-hit data
- notifying the public about the program
- de-identify data for planning, analysis

These best practices can be applied to other smart city initiatives



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 with: These servers contain all the town's data, including fin-

Ontario police warn of recent cyberattacks targeting local governments

THE CANADIAN PRESS Updated: September 14, 2018

Governance and Privacy Controls

Data governance

- effective and independent oversight
- contracts with third parties clearly defining privacy and accountability

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

guard against re-identification of data

Community engagement and project transparency



Security Obligations

FIPPA and MFIPPA

- require government institutions to ensure that reasonable measures are defined, documented and put in place, to protect personal information
- reasonable measures include administrative, technical and physical controls

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
- Four finalist communities from Ontario:
 - Biigtigong Nishnaabeg (Pic River First Nation)
 - City of Guelph and Wellington County
 - Mohawk Council of Akwesasne
 - Region of Waterloo

Information and Privacy Commissioner of Ontario

Office of the Privacy

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

Privacy Commissioner of Newfoundland and Labrador

Office of the Information and Privacy Commissioner of the Northwest Territories

Yukon Information an 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

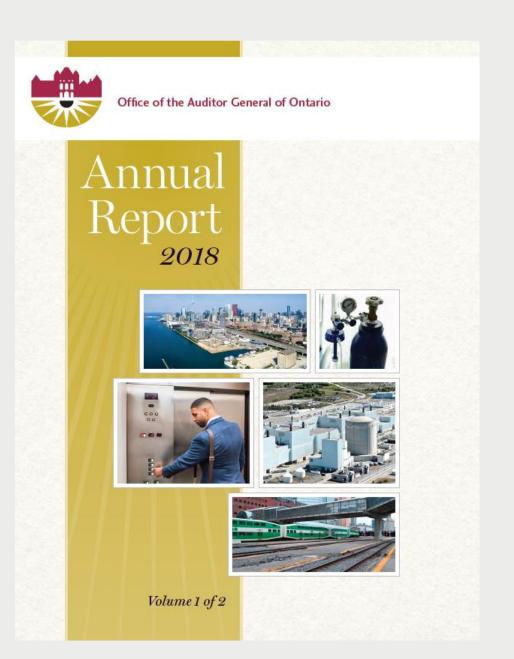
- Sidewalk Toronto would represent North America's largest smart city project
- Sidewalk Labs and Waterfront Toronto preparing Master Innovation and Development Plan
- The IPC will support provincial and municipal stakeholders as they review the plan

Role of the IPC

In her 2018 Annual Report, Ontario's Auditor General recommended that in order to protect the public's interest, a policy framework should be established, "... through legislation, for the development of a smart city in Ontario that addresses intellectual property; data collection, ownership, security and privacy ..."

— Annual Report 2018, Vol. 1, p. 695.

Office of the Auditor General of Ontario



Potential Role of the IPC

Toronto Board of Trade recommended in their report, *BiblioTech*, that the IPC:

- oversee the proposed Data Hub
- be granted the ability to lay fines for misusing data
- have the resources to enforce strict compliance with existing legislation and the Data Hub





