Legal and Privacy Implications of Smart Cities

David Goodis
Assistant Commissioner
Information and Privacy Commissioner of Ontario

Cyber Security 2017: Securing the Smart City of the Future

February 27, 2017

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

Who is the Information and Privacy Commissioner?

- Brian Beamish appointed by Ontario Legislature (March 2015)
  - 5 year term
  - reports to Legislature, not government or minister
  - ensures independence as government "watchdog"

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

Commissioner’s mandate

- Commissioner oversees three statutes:
  - *FIPPA/MFIPPA*: public sector access and privacy (ministry, municipality, police, school board, university, hospital)
  - *PHIPA*: privacy of health information (“HICs”…hospitals, clinics, other health care providers)

Commissioner's Mandate

- Commissioner's oversight role in privacy matters:
    - investigate complaints about government/HIC breach of *FIPPA/PHIPA* privacy rules
        - e.g. improper collection or use, unauthorized disclosure
    - *FIPPA*: report with findings of fact and law, recommendations (Ombudsman-like role)
    - *PHIPA*: binding order with legal/factual findings (must be complied with unless appeal to Divisional Court)

Commissioner’s Mandate

- Commissioner’s oversight role in access matters:
  - if government agency denies access, or gives only partial access
  - appeal to Commissioner, conduct inquiry, may order agency to disclose
  - order final, unless judicial review (*JRPA*)

Commissioner's Mandate

- Commissioner's policy role:
  - comment on proposed legislation, programs that impact privacy/access rights
  - educate through research, publications, public speaking

Presentation Overview

Context

Privacy and Access Issues

Ontario Privacy and Access Laws

Collection

Use/Disclosure

Safeguards

Access

Putting it all Together

Context

- "smart cities" depend on widespread use of sensors, ubiquitous connectivity, almost limitless storage and processing power, i.e. "Big Data"
- real time, accurate data and intelligence from multiple sources
- benefits?
  - o better policy making
  - o enhanced service delivery
  - o revenue generation
  - o improved enforcement

Smart Cities

Examples:

- monitoring social media | citizen reporting apps
- automatic licence plate recognition | enforcement
- real-time traffic maps | parking/transit management
- smart meters | electricity consumption
- public wifi and other communication services
- making data open and available to the public

Privacy/Access Concerns

Lack of transparency

Lack of consent

Surveillance

Profiling

Discrimination

Security risks

Lack of access

Lack of accountability

Privacy Obligations under *MFIPPA*

Collection, use, disclosure rules

No **collection** unless

- authorized by statute
- used for law enforcement or
- necessary to lawfully authorized activity

Must have a legitimate reason for collecting personal information, such as requiring a birth certificate to issue a driver's license

No **use** unless

- purpose collected
- consistent purpose
- written consent

Cannot use information from the birth registry to send out birthday cards

No **disclosure** unless

- consent
- consistent purpose
- comply with legislation
- law enforcement
- health or safety
- compassionate reasons

Video capturing evidence of a crime can be shared with police, even if it contains personal information

Collection

quthority

limits on collection

notice

illustrative guidance:

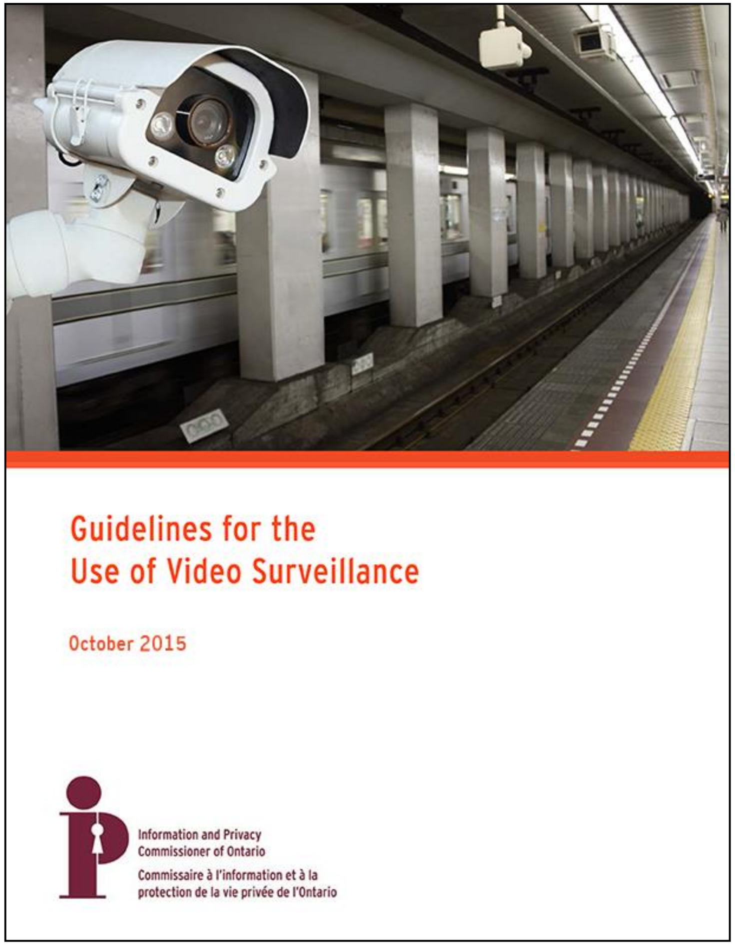
- video surveillance
- body worn cameras

City CCTV Footage

- reporter makes FOI request for camera footage from five locations near scene of fatal bus/train collision
- city identifies five CCTV clips from certain locations that had images (faces) blurred using image blurring technology, but denied access, citing unjustified invasion of privacy
- IPC found blurred video cannot be considered personal information, ordered it to be disclosed

Video Surveillance

- video surveillance captures sensory information about activities and events in a given area
- IPC first published guidelines on the use of video surveillance in public places (2001), then on use in schools (2003)
- IPC's 2015 "Guidelines for the Use of Video Surveillance" provide a list of best practices



Guidelines for the
Use of Video Surveillance

October 2015

Information and Privacy
Commissioner of Ontario

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

Body Worn Cameras

- Body Worn Cameras (BWCs) present different challenges from CCTV and dashboard camera systems
- mobile – increased potential to capture information in various settings like residences, hospitals, places of worship
- must balance transparency, accountability, law enforcement needs and right to privacy
- IPC consulted by the Toronto Police Service on its pilot project, offered recommendations
- “Guidance for the Use of Body-worn Cameras by Law Enforcement Authorities” developed by privacy oversight offices across Canada, including the IPC

Governance Framework For BWCs

- comprehensive framework needed to address privacy and security issues including:
  - when recording will be permitted, required, prohibited (e.g. on/off protocols)
  - retention, use, disclosure and destruction of recordings
  - privacy and security safeguards for cameras, servers, and other systems (e.g. encryption, role-based access, audit processes)
  - responding to access requests (e.g. redaction)
  - specific requirements regarding notifying individuals of the collection of their PI

Use/Disclosure

authority

contracting with third parties

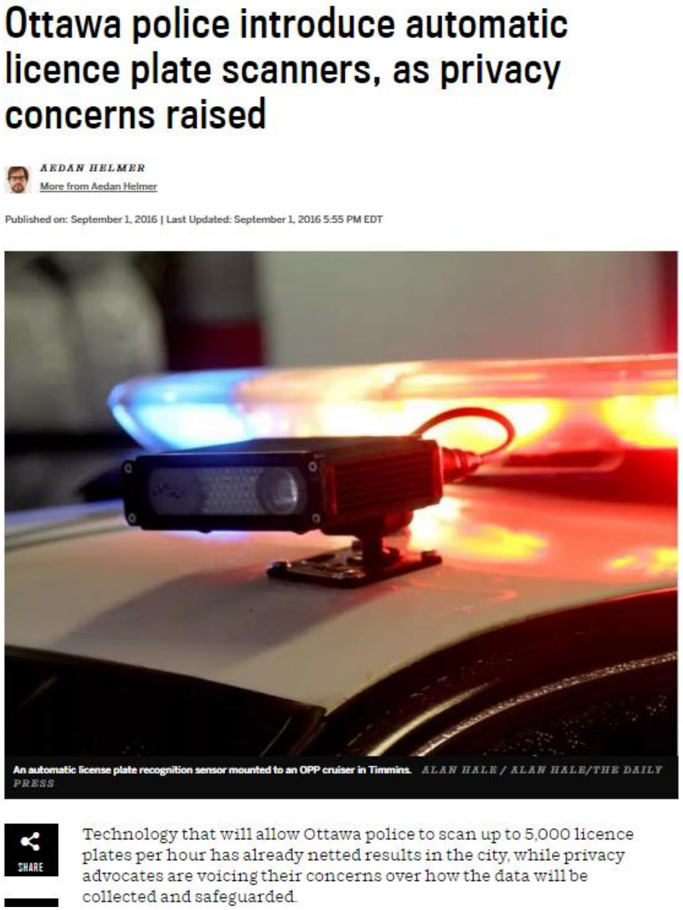
consistent purpose

illustrative guidance:

- automated licence plate recognition (ALPR)
- cloud computing

Licence Plate Recognition

- 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 advice on implementation, best practices for use in a privacy-protective manner



Ottawa police introduce automatic licence plate scanners, as privacy concerns raised

AEDAN HELMER
More from Aedan Helmer

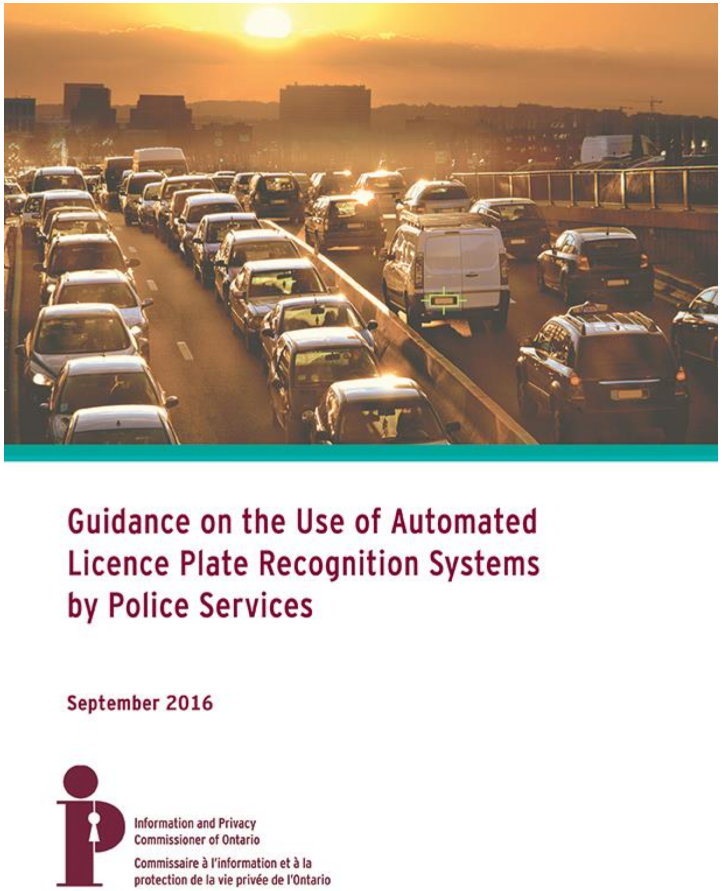
Published on: September 1, 2016 | Last Updated: September 1, 2016 5:55 PM EDT

An automatic license plate recognition sensor mounted to an OPP cruiser in Timmins. *ALAN HALE / ALAN HALE/THE DAILY PRESS*

Technology that will allow Ottawa police to scan up to 5,000 licence plates per hour has already netted results in the city, while privacy advocates are voicing their concerns over how the data will be collected and safeguarded.

Best Practices for ALPR

- 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



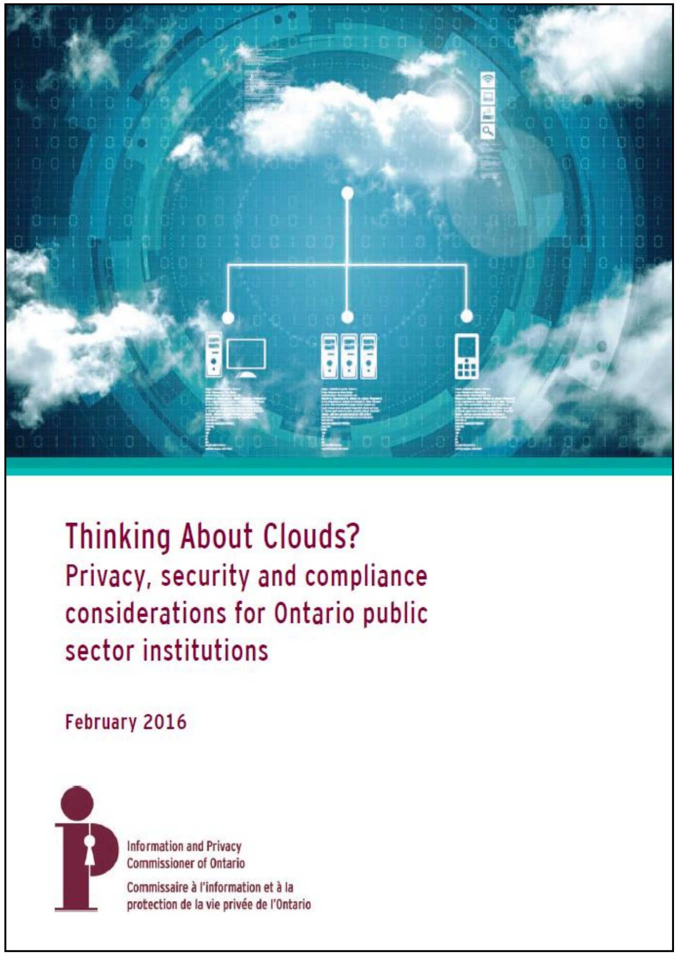
Guidance on the Use of Automated Licence Plate Recognition Systems by Police Services

September 2016

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

Cloud Computing

- evaluate whether cloud computing services are suitable
- identify risks associated with using cloud computing
- outline strategies to mitigate risks



Thinking About Clouds?
Privacy, security and compliance considerations for Ontario public sector institutions

February 2016

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

Clouds
Risks and Mitigation Strategies

Risks

- Unauthorized processing and secondary uses
- Covert surveillance
- Insider threats
- Loss of access
- Identifying applicable law
- Inability to negotiate terms of service

Risk Mitigation Strategies

- Understand your legal and policy obligations
- Conduct a PIA and TRA
- Minimize PI
- Know your cloud service provider
- Negotiate comprehensive and enforceable contracts
- Incident management plan

Safeguards

reasonable safeguards

breach response

penalties and other consequences

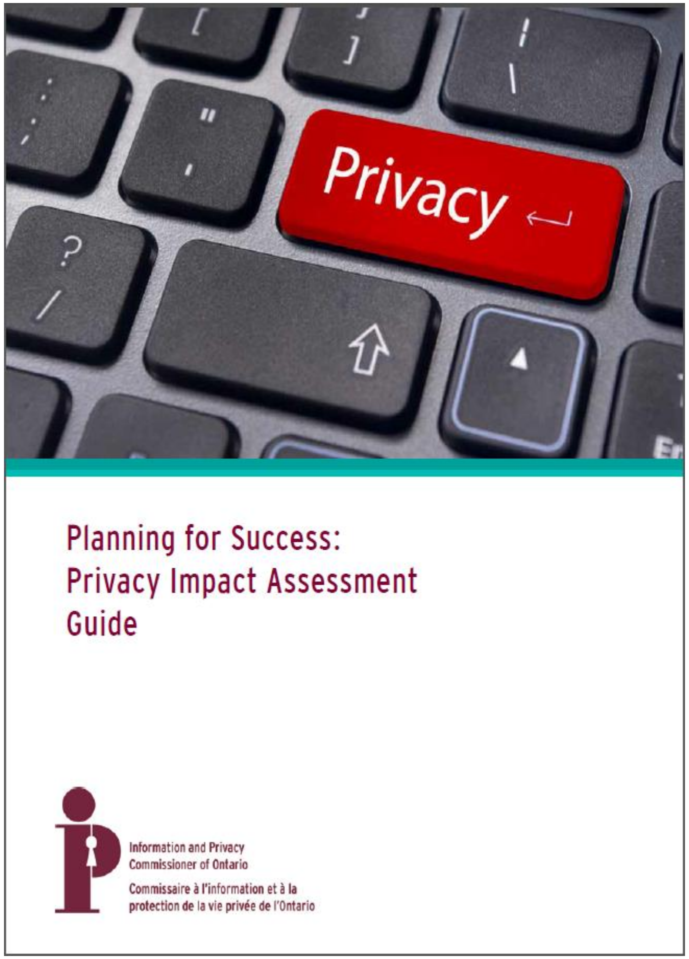
illustrative guidance:

- PIAs/TRAs
- strong encryption
- breach management

Privacy Breaches

- privacy breach occurs when personal information is collected, used or disclosed in ways not consistent with privacy laws
- among most common breaches is unauthorized disclosure of personal information such as:
  - sending communications to wrong recipient due to human error
  - improper record destruction procedure
  - loss or theft of unsecured assets, such as laptops, digital cameras, portable storage devices (USB sticks)
- IPC may investigate privacy complaints, report publicly on them
  - may order government to cease and destroy a collection of personal information
  - may make recommendations to safeguard privacy

Privacy Impact Assessments



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

PIA Guide

- tool to identify privacy effects, mitigate risks, of a given project
- widely recognized as a best practice
- simplified 4-step methodology with tools
- basis for developing internal PIA policies and procedures

Download at: https://goo.gl/9gM1x6

Protecting Against Ransomware

- what is ransomware?
- how do computers get infected?
  - phishing attacks
  - software exploits
- protecting your organization
- responding to incidents

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.

Access

individual rights

Open Government

Open Data

illustrative guidance:

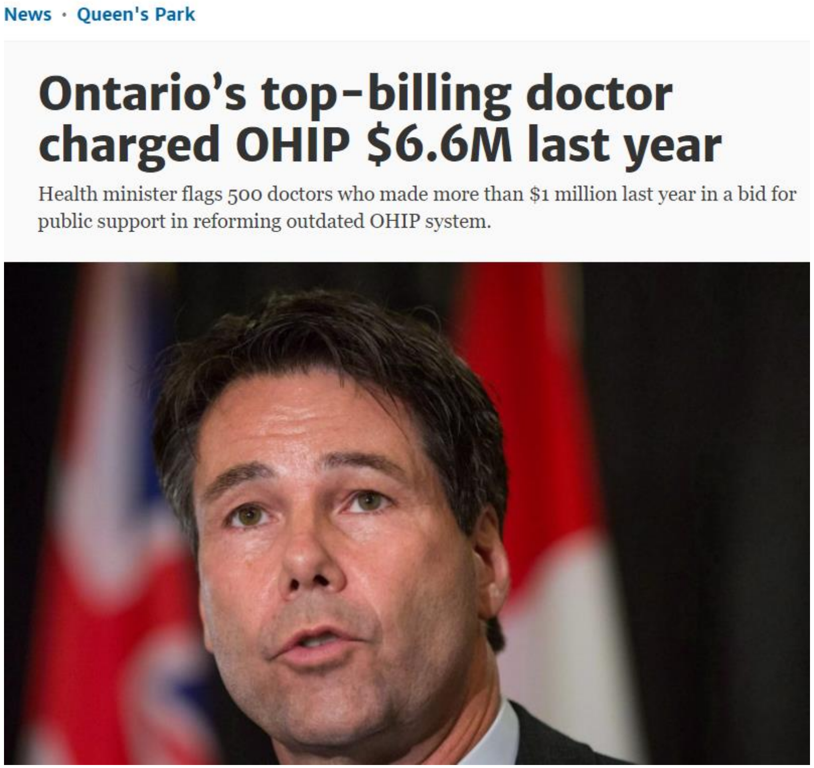
- Government Procurement
- De-identification

Right of Access under *FIPPA/MFIPPA*

- every person has a right of access to a record in the custody or control of an institution with limited exceptions
- any record can be requested (the question “is this FOI-able” is a common one – answer usually “yes” if about government business!)
- requesters can appeal an institution’s decision to the IPC, which can uphold denial of access or order disclosure

Doctor's Billings and Public Interest

- significant public attention about amount doctors bill to public
- previous IPC decisions kept this information private
- recent order, PO-3617, requires disclosure – personal privacy exemption does not apply
- even if it applied, overriding public interest in disclosure given the importance of transparency in use of substantial public money (order currently under judicial review)


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.

Open government – proactive disclosure

Three pillars:

1. Open Data: proactive publication of data in free, accessible forms for public use (e.g. water test results)
2. Open Dialogue: new ways to provide public with a meaningful voice in planning, decision making (e.g. police carding consultations, e-petitions)
3. Open Information: proactive release of information about the operation of government (e.g., contracts)

Proactive disclosure

- Open Government supports, expands *FIPPA* right of access
- more than just reactive disclosure (in response to access request)
- government information should be made public in anticipation of, and in response to, the public's needs and interests, unless there are legitimate legal, privacy, security, confidentiality reasons not to
- Open by Default is a presumption in favour of disclosure over non-disclosure, mirrors *FIPPA*'s over-arching access principles

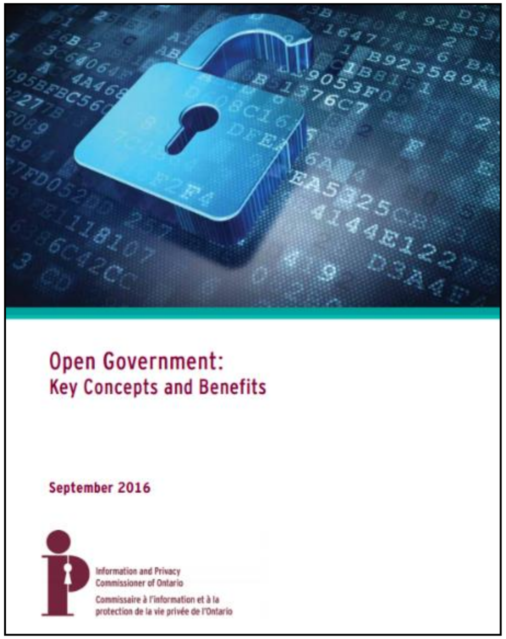
Open Cities Index

- Public Sector Digest ranked the Open Data programs of 34 Canadian municipalities:
  - Toronto #2
  - Ottawa #4
  - London #5
  - Windsor #8
  - Oakville #9

IPC Efforts

- IPC works with organizations to advance Open Government
- reaching out to institutions to learn from their experience (Guelph)
- participate in a municipal-lead Open Government Community of Practice.
- developing practical guidance papers to help all institutions to begin or expand their Open Government programs

Open Government: Key Concepts and Benefits



Open Government:
Key Concepts and Benefits

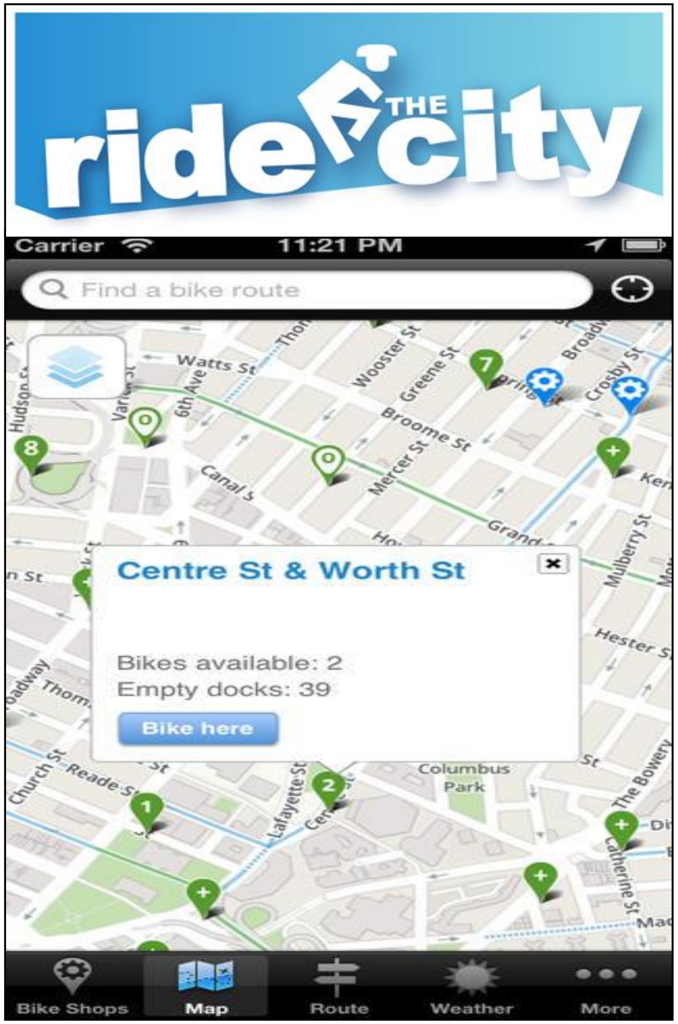
September 2016

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

- introductory, summarizes fundamental concepts and benefits, draws together variety of sources to facilitate understanding of Open Government
- highlights two significant goals:

1. Enhancing transparency to improve the quality of governance and services by becoming more open, accountable, and responsive to the public
2. Enhancing public engagement to enable broad participation and true two-way dialogue, resulting in more "citizen centric" information and services

Apps Made in Ontario from Open Data

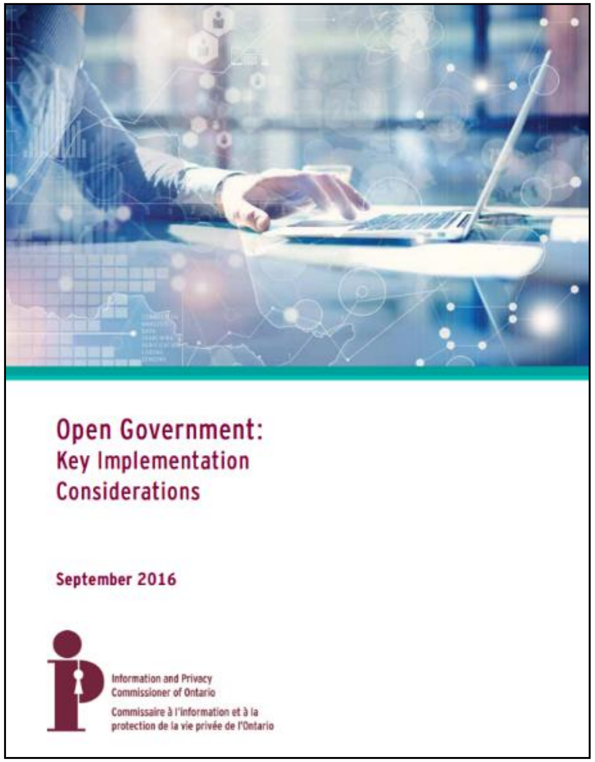


Centre St & Worth St

Bikes available: 2
Empty docks: 39

Open Government: Key Implementation Considerations

- overview of important considerations when implementing OG
- key factors for success:
  - recognizing OG is an ongoing program, not short-term project
  - making sure institution has leadership, commitment, governance, resources to sustain program
  - defining scope and deliverables realistically, appropriate for institution
  - engaging users and public as institution plans, implements and evaluates its activities and services



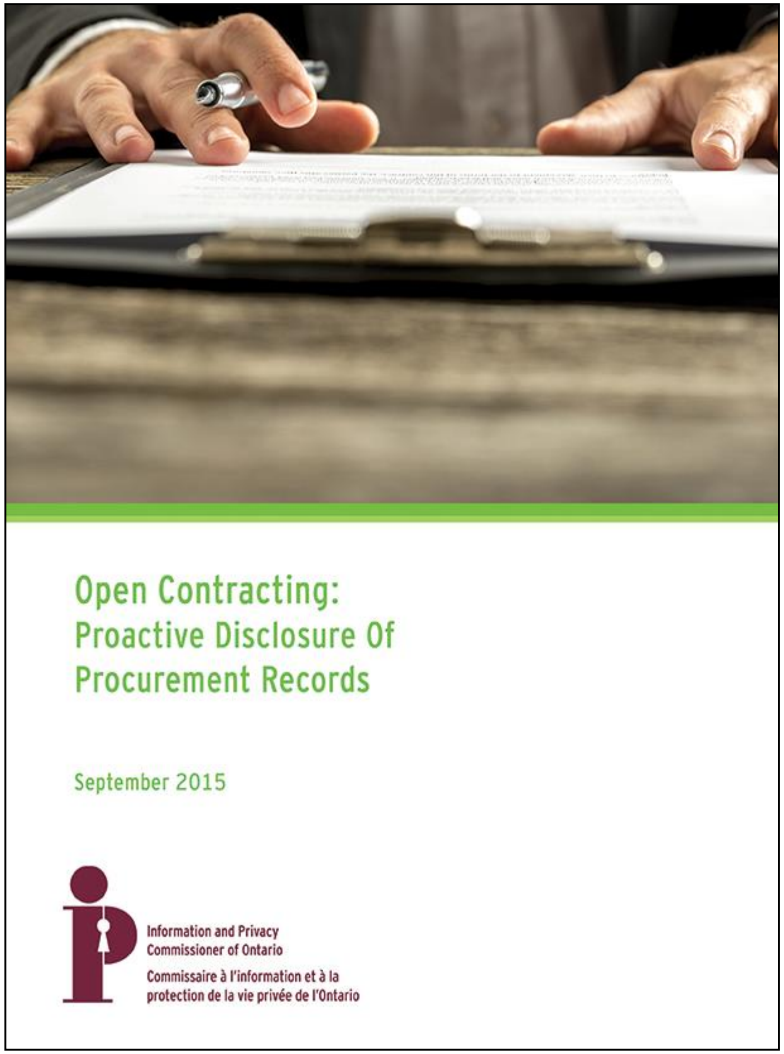
Open Government:
Key Implementation
Considerations

September 2016

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

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

Open Government, Open Contracting



Open Contracting: Proactive Disclosure Of Procurement Records

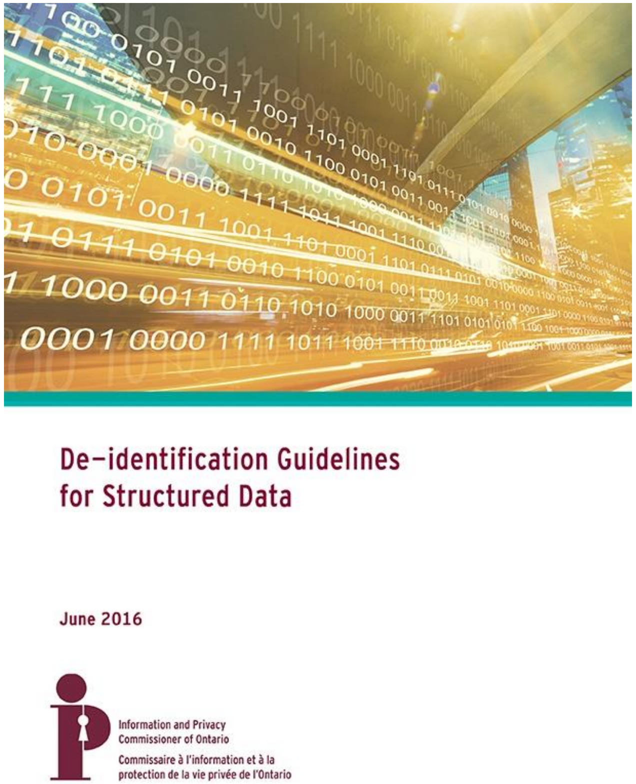
September 2015

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

- Proactive disclosure of procurement records will improve the **transparency of government spending** and reduce resources required to respond to access to information requests.
- This paper provides guidance on how to make procurement records publically available, while protecting sensitive **third party information** and **personal information**.

De-identification Supports Open Government

- “De-identification” - process of removing PI from a record or data set
- outlines a risk-based, step-by-step process to assist institutions in de-identifying data sets containing PI
- covers key issues to consider when publishing data:
  - *release models*
  - *types of identifiers*
  - *re-identification attacks*
  - *de-identification techniques*



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

Information and Privacy Commissioner of Ontario

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

Putting it all together

Big Data/

Data Integration

Data Integration

- sometimes known as data linking or computer matching
- involves the computerized comparison of databases to allow linkages to be made with information
- technology has changed the landscape
- where the data integration involves PI, there is a requirement to comply with *FIPPA* and *MFIPPA*

Privacy Challenges of Data Integration

- PI should be collected directly from the individual
- Normally should only be used and disclosed for the purpose for which it was collected or a consistent purpose
- subject individual has a right to notice of the collection
- PI used by an institution should not be used unless it is accurate and up to date

Big Data Analytics

- process of running algorithms on integrated data sets to uncover hidden patterns
- use may raise significant privacy and other ethical and fairness concerns
- may be used to infer rules that allow for automated decision making (about individuals) and the prediction of future results
- process works the same regardless of whether analyzed data sets are de-identified, although the patterns extracted may differ

Recent Initiatives

- data integration initiatives differ from past ones
- purpose is to support policy development, system planning, resource allocation, performance monitoring
- although not tied to direct service delivery, research may inform future collection and use of PI
- challenge is to ensure adequate measures to protect individuals whose PI is collected, used, disclosed, while enabling the initiatives

Privacy Risks of Big Data

- generation of new PI not collected directly from the individual
- use of poorly selected data sets that:
    - lack information/are incomplete
    - contain incorrect or outdated information
    - disproportionately represent certain populations
- incorporation of implicit or explicit biases
- generation of pseudo-scientific insights that assume correlation equals causation
- lack of knowledge/transparency regarding the inner “logic” of the system
- ***if not designed properly, can result in uses of PI that may be unexpected, invasive and discriminatory***

Best Practices

- legislative authority to collect, use and disclose PI within and among institutions
- independent review process to govern projects including PIAs, TRAs, research ethics
- prohibit use of sensitive categories of PI
- transparency of approved projects
- secure process for linking PI
- requirement to de-identify PI after linking
- delete the linked data once the research is complete

Additional Safeguards

- provide notice to affected individuals
- allow affected individuals to challenge or respond to the results

Governance and Oversight

- accountability frameworks for data integration and big data analytics should involve senior staff with authority to monitor and provide effective oversight
- projects should engage experts in human rights, research ethics, privacy and de-identification

The IPC'S Open Door Policy

- achieving balance we are striving for is not possible without the involvement of other agencies and stakeholders
- IPC has an **open door policy** for any Ontario institution considering programs which may impact privacy
- we believe that the 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

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