Big Data and Other Developments in the Public Sector

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

Lexpert 9th Annual Information Privacy and Data Protection

November 30, 2017

Who is the Information and Privacy Commissioner?

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

Ontario's Legislative Framework

Public Sector	Health Sector	Private Sector
Freedom of Information and Protection of Privacy Act (*FIPPA*) 300+ **provincial institutions** e.g. ministries, agencies, boards, hospitals, universities *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*) 1200+ **local bodies** e.g. municipalities, police, school boards, hydro	*Personal Health Information Protection Act* (*PHIPA*) Individuals and organizations delivering **health care services** e.g. hospitals, pharmacies, laboratories, doctors, dentists, nurses	*Personal Information Protection and Electronic Documents Act* (*PIPEDA*) **Ontario private sector** organizations e.g. businesses (including banks, and not-for-profits) engaged in **commercial activities**
IPC oversight	IPC oversight	Privacy Commissioner of Canada oversight

Mission and Mandate

MISSION: We champion and uphold the public's right to know and right to privacy

MANDATE:

- resolve access to information appeals and privacy complaints
- review and approve information practices
- conduct research, deliver education and guidance on access and privacy issues
- comment on proposed legislation, programs and practices

Big Data in the Public Sector

What is Big Data?

- **shift** in how we think about and use data
  - new combinations of data may contain useful but hidden patterns
  - analytics can discover these insights
- **technology advancements**
  - new sources and methods of data collection
  - almost unlimited storage capacity
  - better linkage techniques
  - algorithms that learn from and make predictions on data

Big Data and *FIPPA/MFIPPA*

- Ontario public sector, like all governments, want to jump in!
  - public benefits to research, system planning, allocating resources
- unfortunately, big data can result in uses of PI that are unexpected, invasive, inaccurate, discriminatory or disrespectful of individuals

Big Data and *FIPPA/MFIPPA*

- Ontario public sector legislation not designed to cope with big data:
  - web not yet invented
  - information technology was less prevalent
  - types of data and analytics were less complex
  - uses of personal information were discrete and determinate
- current legislative framework treats government institutions as silos
  - collection of personal information must be “necessary”
  - secondary uses are restricted
  - information sharing is limited

Big Data and *FIPPA/MFIPPA*

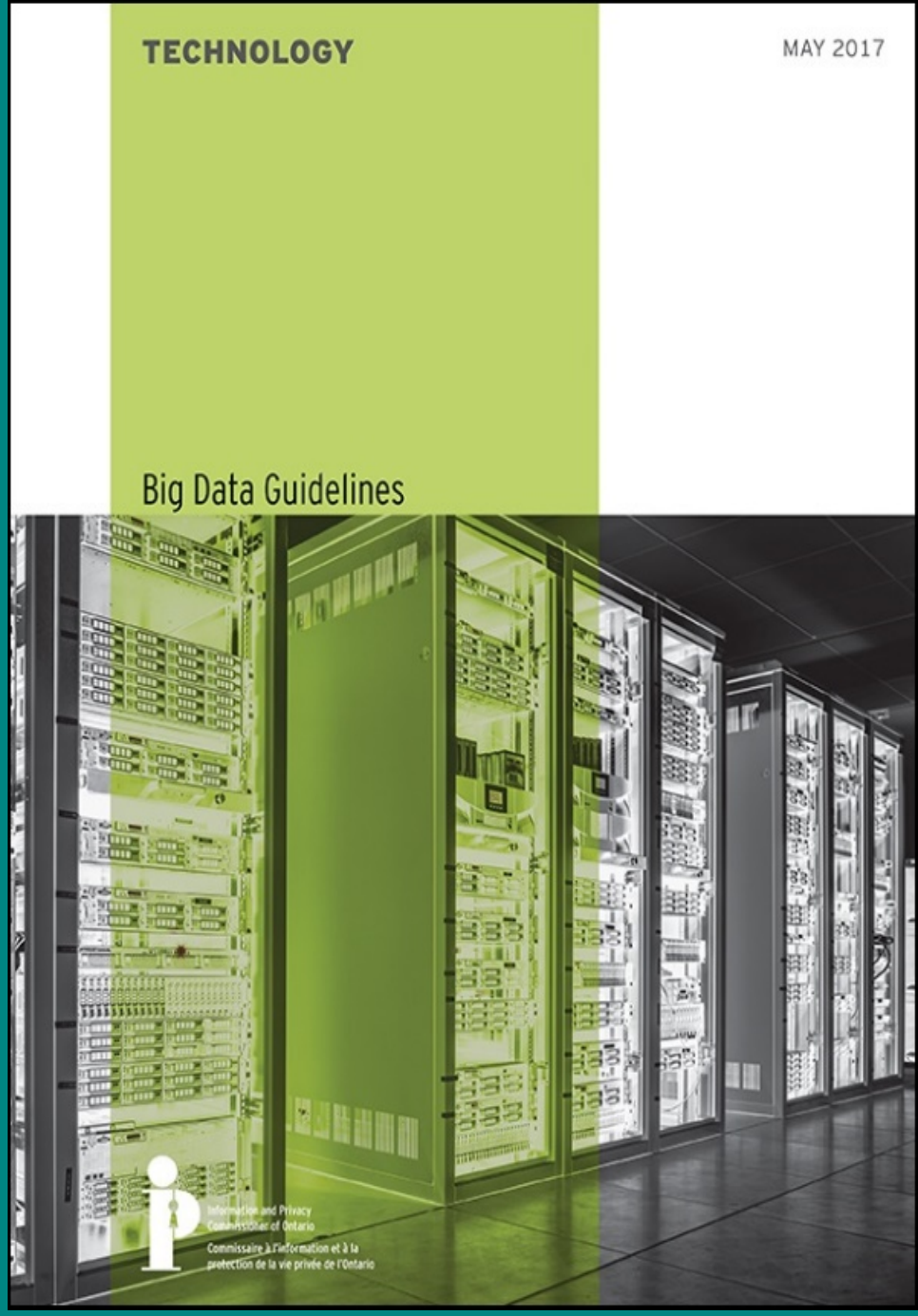
- may still be possible to conduct big data under *FIPPA* if:
  - collection **expressly authorized by statute** [s. 38(2)]
  - disclosure for purpose of **complying with a statute** [s. 42(1)(e)]
- unfortunately, we see piecemeal approach – ministries request IPC approval of specific projects, or ministry-specific legislation

Big Data and *FIPPA/MFIPPA*

- to support big data in general, we need a **new Ontario government-wide legislative framework**
  - single dedicated unit in OPS to collect PI from other ministries, link, de-identify
  - then provide de-identified data to ministries to enable them to analyse
  - strong oversight by IPC of this unit
  - built-in ethical review
  - transparency to public!

IPC's Big Data Guidelines

- May 2017
- key issues, best practices when conducting big data projects
- four stages: collection, integration, analysis, profiling
- each stage raises a number of concerns
- institutions should avoid uses of PI that may be **unexpected, invasive, inaccurate, discriminatory or disrespectful** of individuals



Big Data: Private vs. Public Sector

- big data responsibilities may differ in private and public sectors
- each sector has different set of considerations:
  - authority for collection
    - private sector – authority mostly from **consent**
    - public sector – authority mostly from **necessity**
  - choice of service provider
    - private – clients usually have **choice** of provider
    - public – usually **no choice**

Big Data: Private vs. Public Sector

- important to note **application of *Charter***:
  - private sector – no
  - public sector – yes
- public sector:
  - lack of consent, lack of choice and *Charter* application suggest **greater obligation** to protect personal information while using big data

Privacy Threats

Common Privacy Breaches

1. Insecure disposal of records
   - records in paper format intended for shredding are recycled
   - insecure disposal of hard drives
2. Mobile and portable devices
   - lost or stolen, unencrypted devices such as laptops, USB keys
3. Unauthorized access
   - snooping by otherwise authorized staff, malware (e.g. ransomware)

Ransomware

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

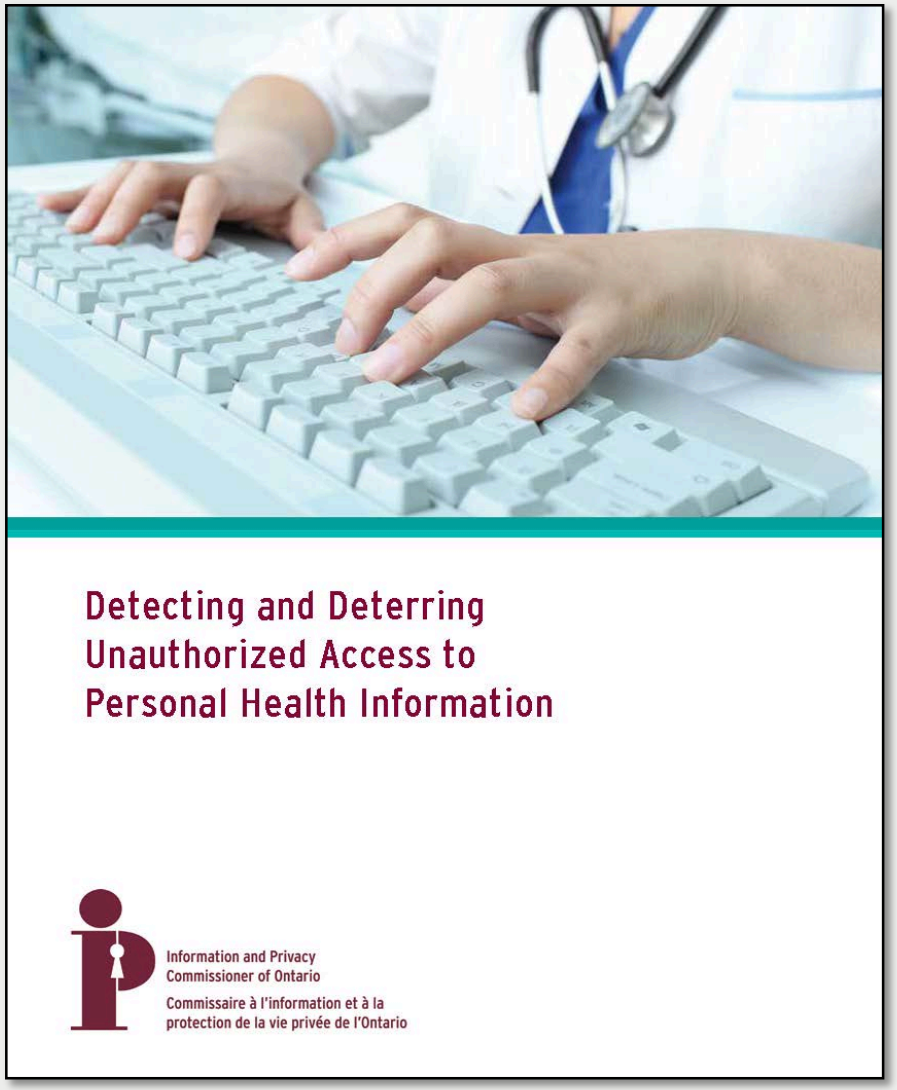
Phishing is a type of online attack in which a hacker sends one or more individuals an unsolicited electronic communication—email, social media post or instant messenger chat—designed to trick or deceive a recipient into revealing sensitive information or downloading malware.

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.

- what is ransomware?
- how computers get infected
  - phishing attacks
  - software exploits
- how to protect your organization
  - administrative, technological measures e.g. employee training, limiting user privileges, software protections
- how to respond to incidents

Snooping Guidance

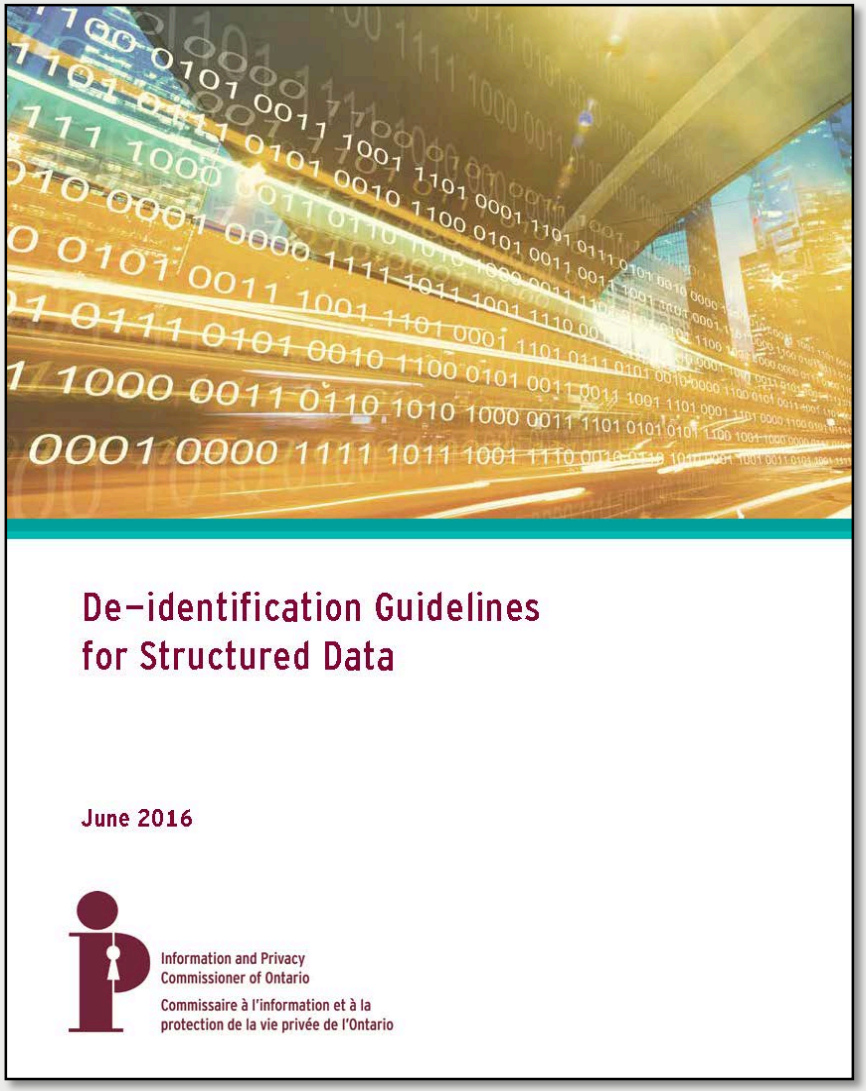


- Guidance outlines
  - impact of unauthorized access
  - how to reduce risk:
    - policies and procedures
    - training
    - privacy notices and warning flags
    - confidentiality agreements
    - access management
    - logging, auditing, monitoring
    - privacy breach management
    - discipline

Reducing Risk of Privacy Breaches

De-identification

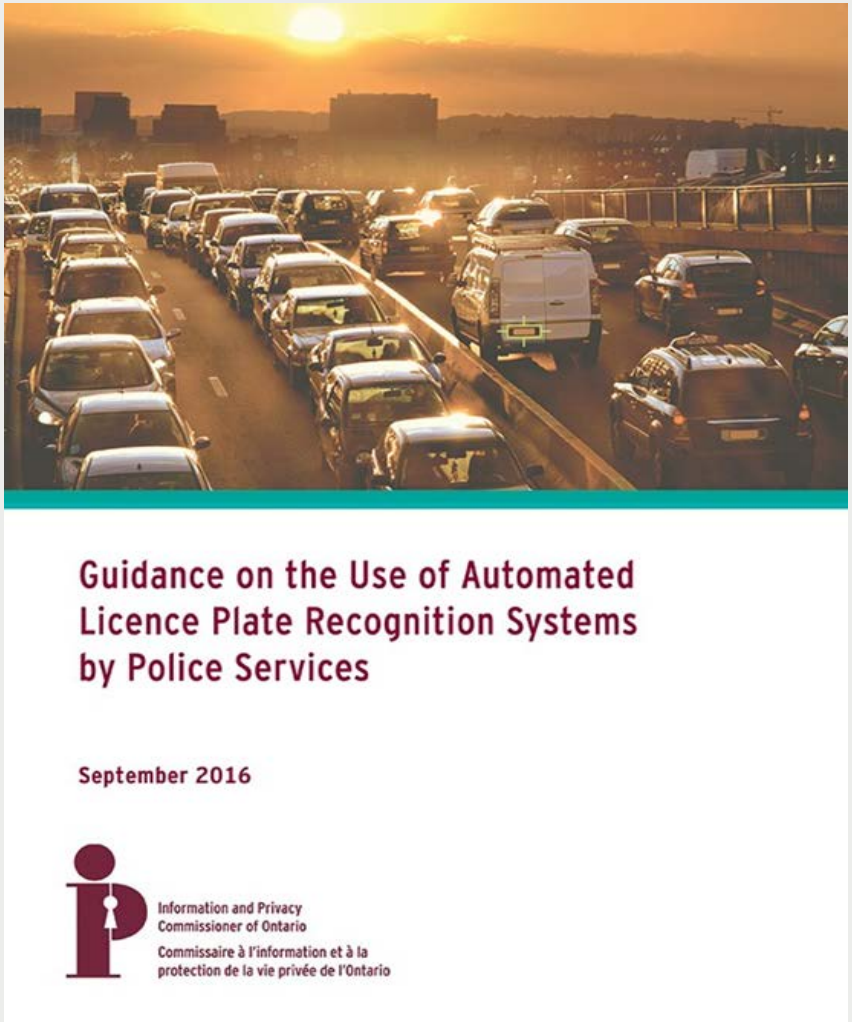
- key issues when de-identifying personal information in the form of structured data
- risk-based, step-by-step process to assist organizations to de-identify
- key issues when publishing
  - release models
  - types of identifiers
  - re-identification attacks
- IPC won global privacy award for excellence in research (International Conference of Data Protection and Privacy Commissioners, Hong Kong 2017)



Reducing Risk of Privacy Breaches Best Practices

Administrative	Technical	Physical
• privacy and security policies and procedures • auditing compliance with rules • privacy and security training • data minimization • confidentiality agreements (alone or part of broader contracts) • other means of communicating privacy messages (privacy notices, warning flags) • PIAs	• strong authentication and access controls • detailed logging, auditing, monitoring • strong passwords, encryption • patch and change management • firewalls, hardened servers, intrusion detection and prevention, anti-virus, anti-spam, anti-spyware • protection against malicious and mobile code • threat risk assessments, ethical hacks	• controlled access to premises • controlled access to locations within premises where identifying information is stored • access cards and keys • identification, screening, supervision of visitors **NOTE –** when determining appropriate safeguards consider • sensitivity and amount of information • number and nature of people with access to the information • threats and risks associated with the information

Law Enforcement: Automated Licence Plate Recognition (ALPR)



- ALPR can quickly capture and match large volumes of licence plate numbers to lists of plates stored in a database
- guidance includes advice on implementation and best practices in using these systems in a privacy-protective manner
- Best practices include
  - **limiting retention** – delete non-hit data as soon as practicable
  - comprehensive **governance framework**
  - **policies and procedures** to ensure the appropriate handling of personal information
  - providing **notice** to the public

Law Enforcement

R. v. Orlandis-Habsburgo (ONCA 2017)

- **police investigating suspected marijuana grow-op**
- hydro company and police have on-going exchange of information about the home and its occupants
- court rules police should have obtained warrant, since reasonable expectation of privacy in electricity usage
- failure to obtain judicial authorization breach of *Charter*, s. 8 unreasonable search and seizure
  - evidence admitted anyway because police believed entitled to data without a warrant

How to Respond to Privacy Breach

Key Steps for Responding to a Privacy Breach

1. Contain Breach
   - initial investigation
   - notification of police, if theft or other criminal activity
2. Evaluate the Risks
   - personal information involved?
   - cause and extent of breach
   - individuals affected
   - possible harm?
3. Notify
   - affected individuals
   - Privacy Commissioner
4. Prevent Future Breaches
   - security audit
   - review of policies and practices, staff training, third party service contracts

OPC Resource: Key Steps for Organizations in Responding to Privacy Breaches
https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gl_070801_02/

What to do When Faced with a Privacy Breach

- *PHIPA* sets out the rules that health information custodians must follow when collecting, using, disclosing, retaining and disposing of personal health information
- guidance to health information custodians when faced with a privacy breach

Commissioner’s Response to Privacy Breach

IPC Breach Reporting

- no mandatory breach reporting to IPC under *FIPPA/MFIPPA*
- mandatory breach reporting to IPC for health information as of October 1, 2017
  - s. 12(3) of *PHIPA* and related regulations
- we receive reports under all three statutes
  - 102 public sector self-reported (2016)
  - 233 health sector self-reported (2016)
  - more learned from complainants, media

What Happens when the IPC Reviews a Breach

- IPC may:
  - ensure adequate containment, notification
  - interview appropriate individuals
  - review the organization's position on the breach
  - ask for status report of actions taken by the organization
  - review and give advice on current policies
  - report with recommendations (rarely order)

Questions?

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