A Deep Dive into the Privacy Landscape

David Goodis

Assistant Commissioner
Information and Privacy Commissioner of Ontario

Canadian Institute Advertising & Marketing Law

January 22, 2018

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
Government organizations e.g. 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*)	Individuals, organizations delivering health care e.g. hospitals, pharmacies, labs, doctors, dentists, nurses *Personal Health Information Protection Act* (*PHIPA*)	Private sector businesses engaged in commercial activities *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)
IPC/O oversight	IPC/O 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:

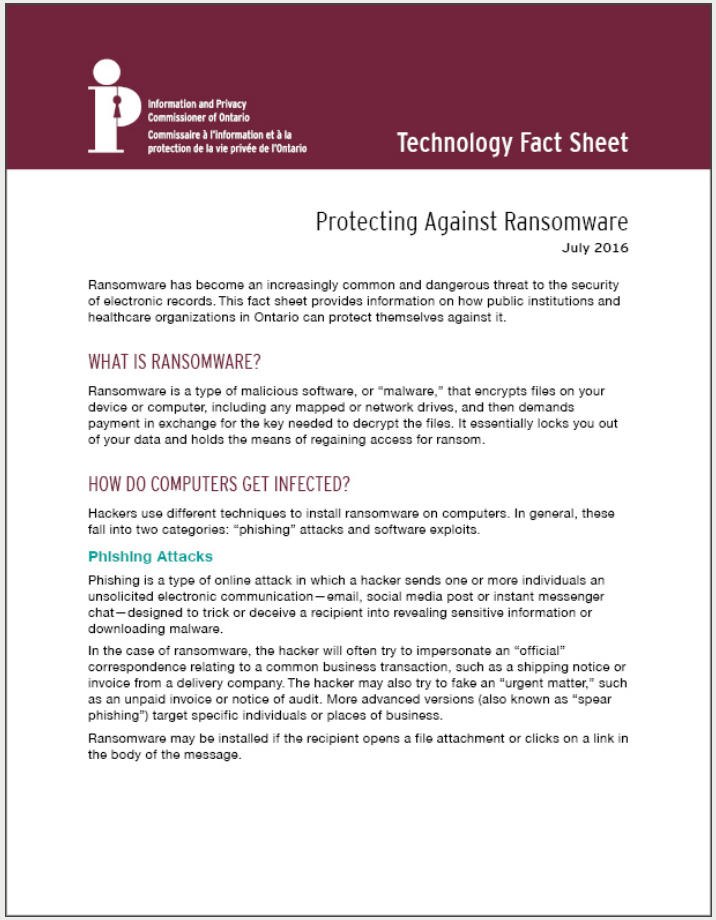
- resolve access to information appeals and privacy complaints
- review and approve information practices
- conduct research, deliver education and guidance on access and privacy issues
- comment on proposed legislation, programs and practices

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

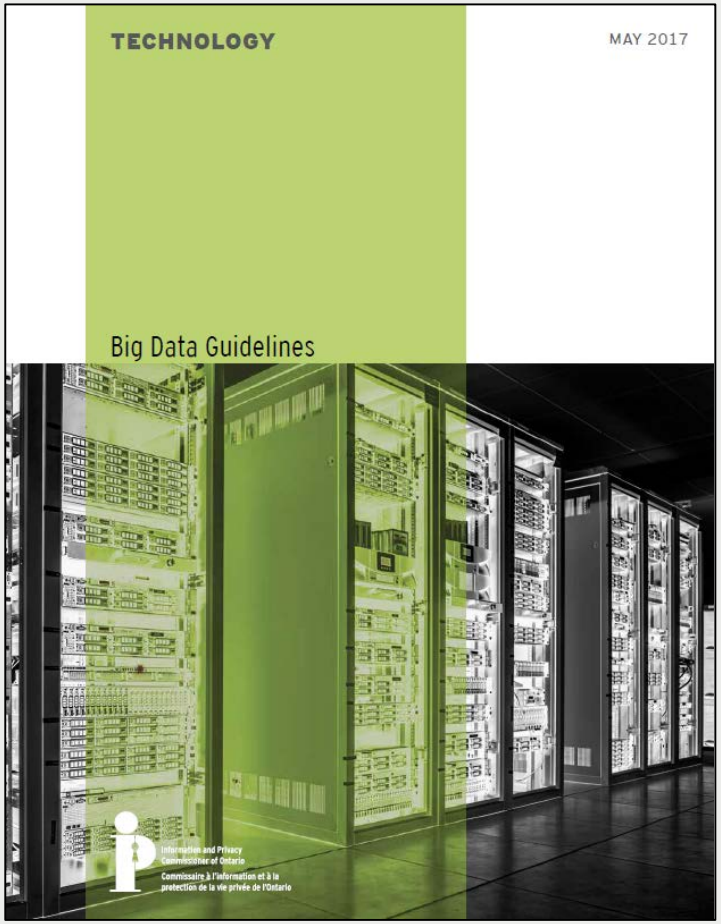
Phishing is a type of online attack in which a hacker sends one or more individuals an unsolicited electronic communication—email, social media post or instant messenger chat—designed to trick or deceive a recipient into revealing sensitive information or downloading malware.

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

Big Data

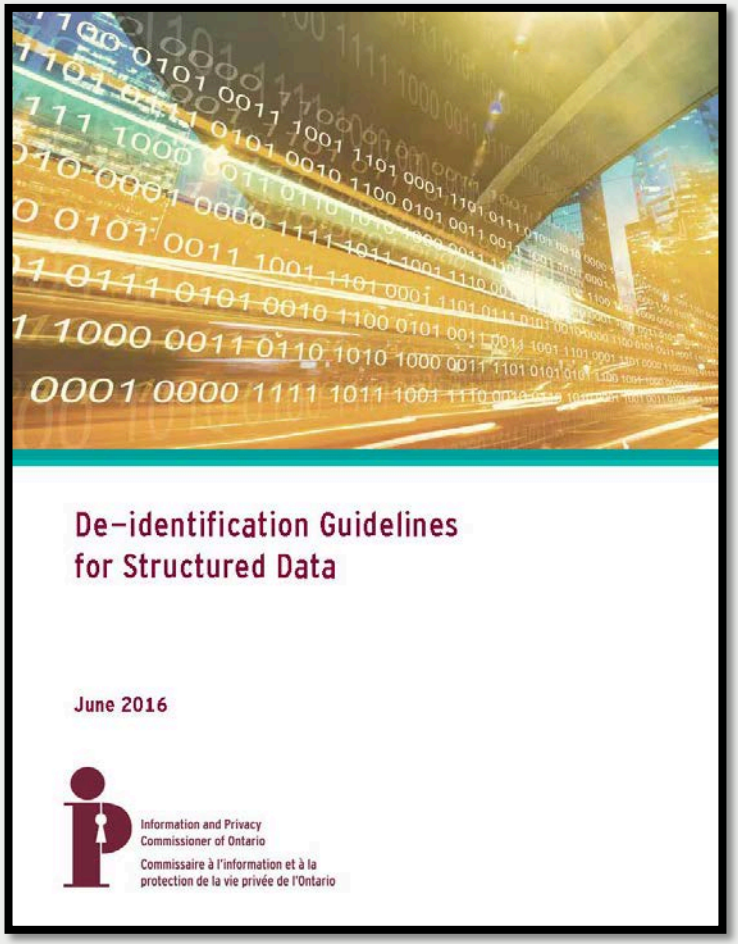


- key issues and best practices when conducting big data initiatives involving personal information
- considerations for each stage of a big data project, including
  - collection
  - integration
  - analysis
  - profiling

Reducing Risk of Privacy Breaches

De-identification

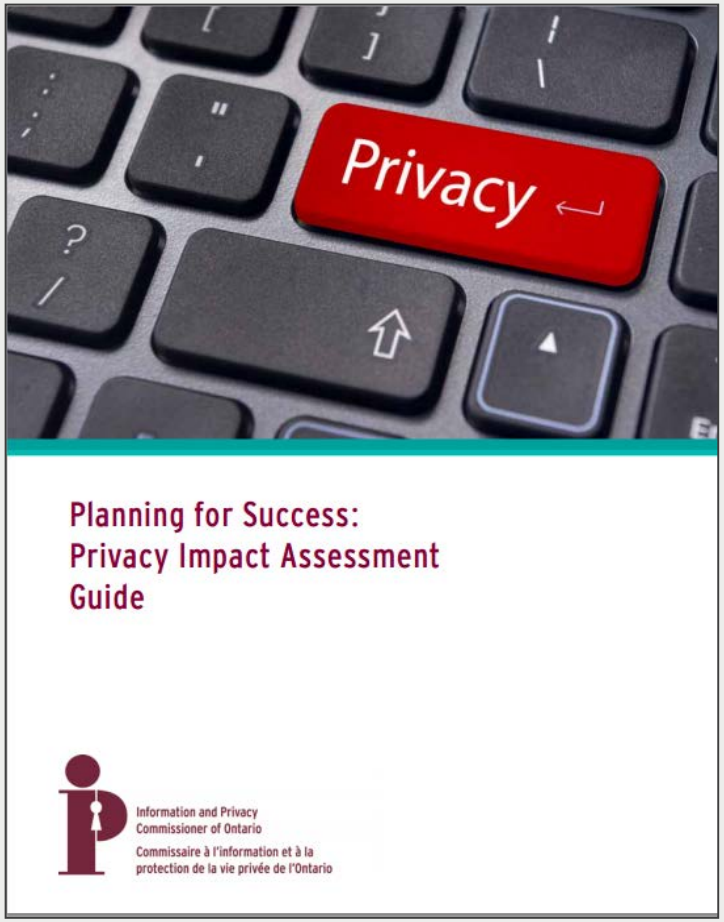
- key issues when de-identifying personal information
- risk-based, step-by-step process to assist organizations to de-identify
- key issues when publishing
  - release models
  - types of identifiers
  - re-identification attacks
- IPC wins global privacy award for excellence in research (International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



Reducing Risk of Privacy Breaches Best Practices

Administrative	Technical	Physical
• privacy and security policies • auditing compliance with rules • privacy and security training • data minimization • confidentiality agreements • Privacy Impact Assessments	• strong authentication and access controls • detailed logging, auditing, monitoring • strong passwords, encryption • patch and change management • firewalls, anti-virus, anti-spam, anti-spyware • protection against malicious code • Threat Risk Assessments, ethical hacks	• controlled access to premises • controlled access to locations within premises where PI is stored • access cards and keys • ID, 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

Planning for Success: Privacy Impact Assessment Guide



- tools to identify privacy impacts and risk mitigation strategies
- step-by-step advice on how to conduct a PIA
- not required by legislation, but considered privacy best practice

How to Respond to Privacy Breach

Responding to a Privacy Breach

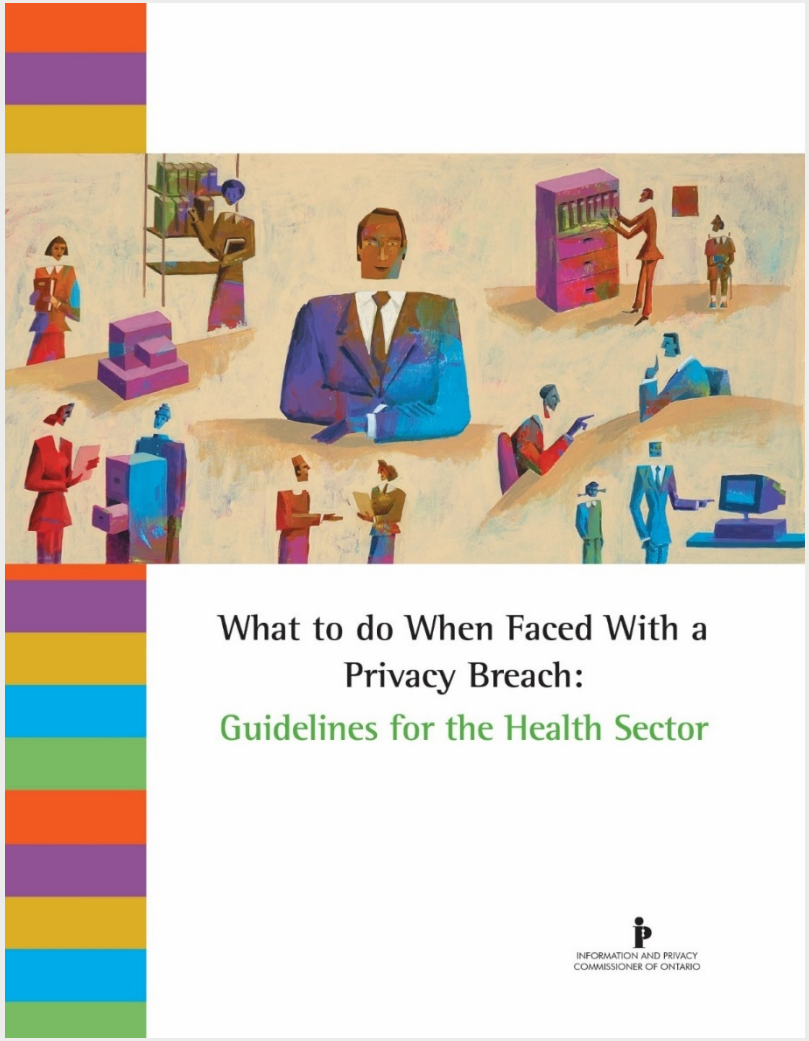
1. Contain Breach
   - initial investigation
   - notify police if theft or other criminal activity
2. Evaluate Risks
   - personal information involved?
   - cause and extent of breach
   - individuals affected
   - possible harm?
3. Notify
   - affected individuals
   - Privacy Commissioner
4. Prevent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

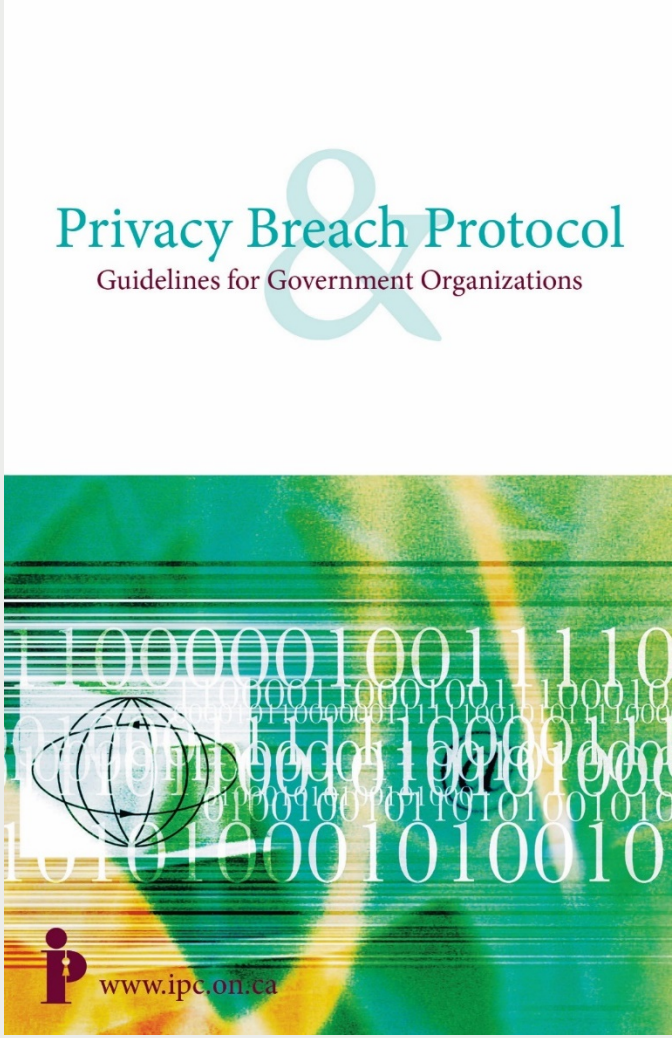
What to do When Faced with a Privacy Breach

- *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



Privacy Breach Protocol Guide

- implementing a privacy breach protocol, as a best practice, helps identify privacy risks, potential and actual breaches
- guidance on what organizations should do when faced with a 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