Canadian Institute
Privacy and Security Compliance Forum

Update from the Ontario Information and Privacy Commissioner

David Goodis
Assistant Commissioner
Ontario Information and Privacy Commissioner
January 31, 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”

Commissioner's Mandate

- Commissioner oversees three statutes:
  - *FIPPA/MFIPPA*: public sector access (FOI) and privacy (ministry, municipality, police, school board, university, hospital)
  - *PHIPA*: privacy of health information
- Commissioner's tribunal role in access matters:
  - if government agency denies access to document, or gives only partial access
  - appeal to Commissioner, who can conduct inquiry, order agency to disclose document
  - order is final, unless judicial review (*JRPA*)

Commissioner's Mandate

- Commissioner's tribunal role in privacy matters:
  - investigate complaints about government/HIC breach of *FIPPA/PHIPA* privacy rules
    - e.g. improper collection, use, disclosure
    - can be on Commissioner's "own motion"
  - *FIPPA*: report with findings of fact and law, recommendations (no JR or appeal; Ombudsman-like role)
  - *PHIPA*: binding order with legal/factual findings (must be complied with unless appeal to Divisional Court)

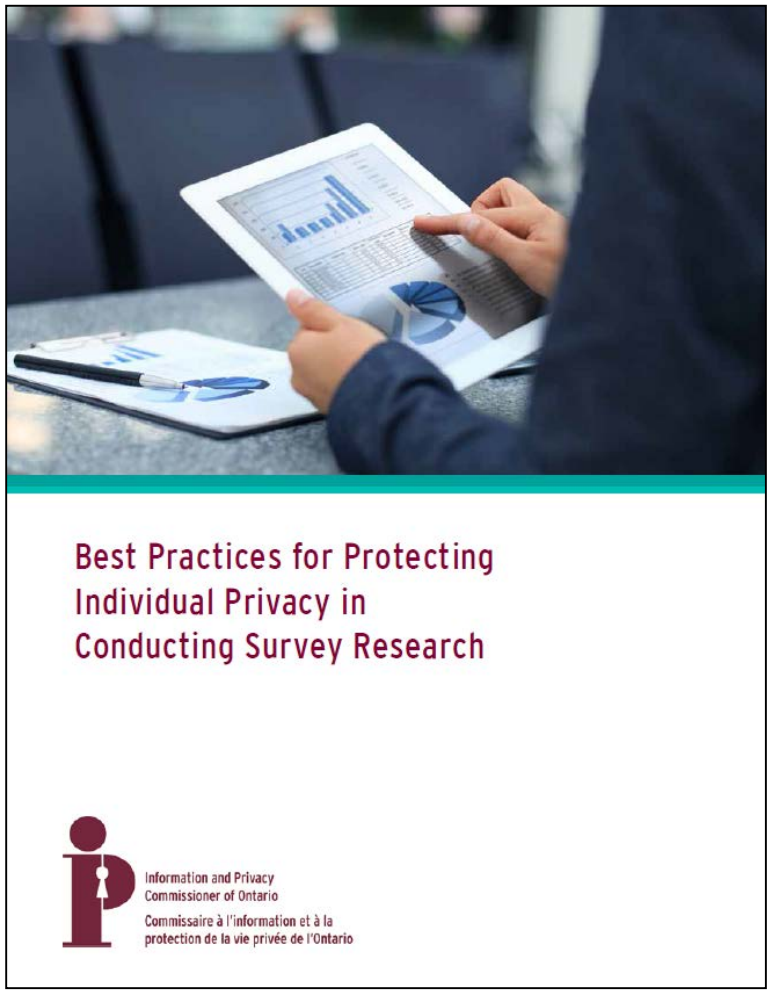
Commissioner's Mandate

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

Doctor's Billings

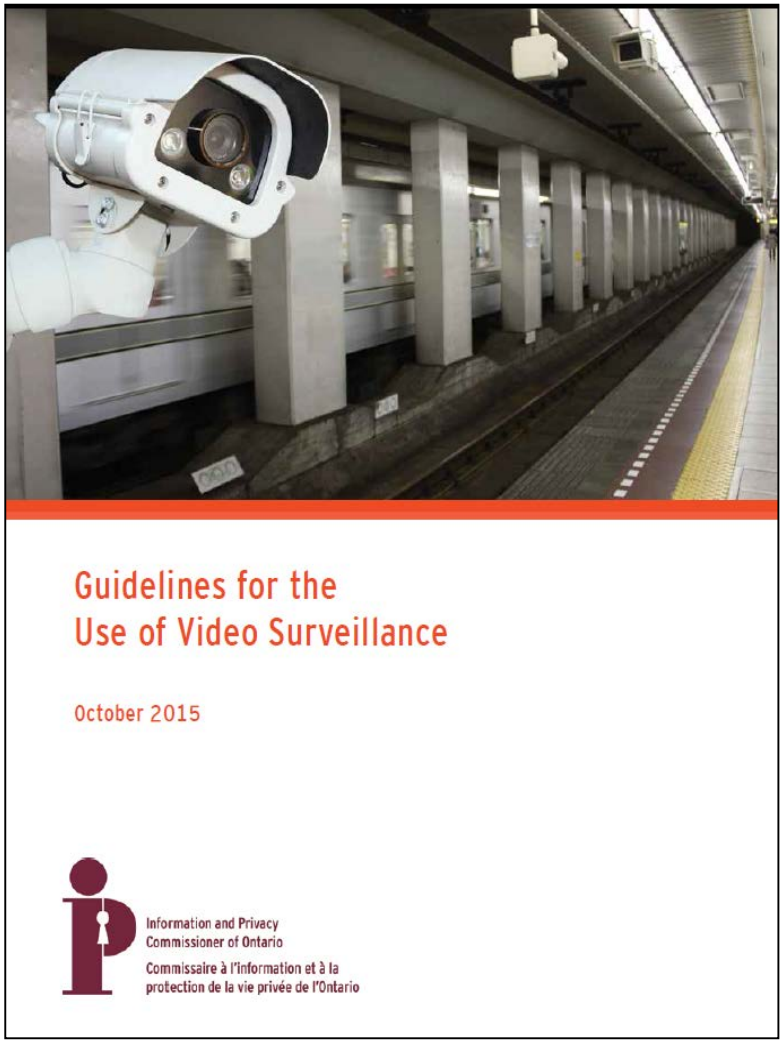
- significant public attention about amount doctors bill to public
- previous IPC decisions kept this information private
- recent order, PO-3617, requires disclosure – personal privacy exemption does not apply
- even if it applied, overriding public interest in disclosure given the importance of transparency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

Privacy: Survey Guidelines



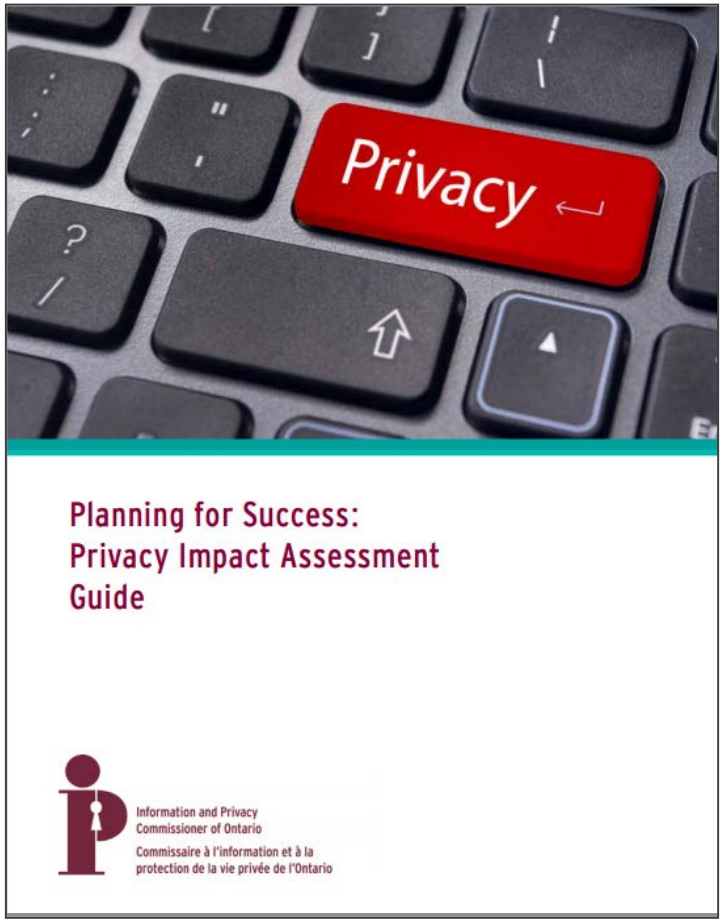
- updated from 1999 version, co-authored with OPS
- changes reflect use of online survey tools, use of mobile devices

Privacy: Video Surveillance Guidelines



- update and consolidation of two older papers

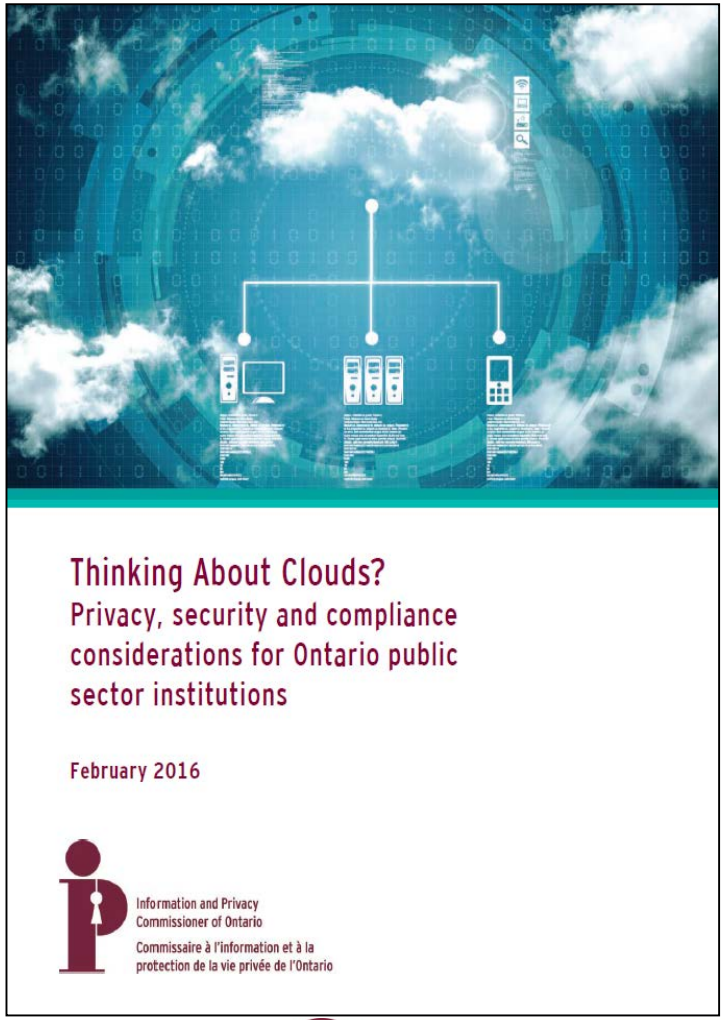
Planning for Success: Privacy Impact Assessment Guide



- tools to identify privacy impacts and risk mitigation strategies
- step-by-step advice on how to conduct a PIA

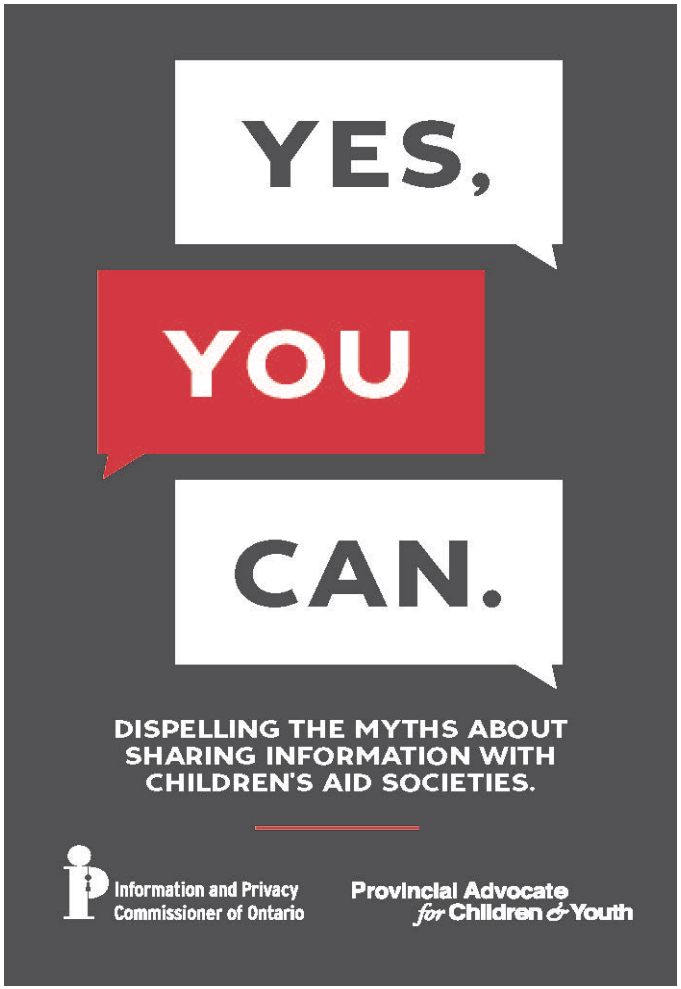
Thinking About Clouds?

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

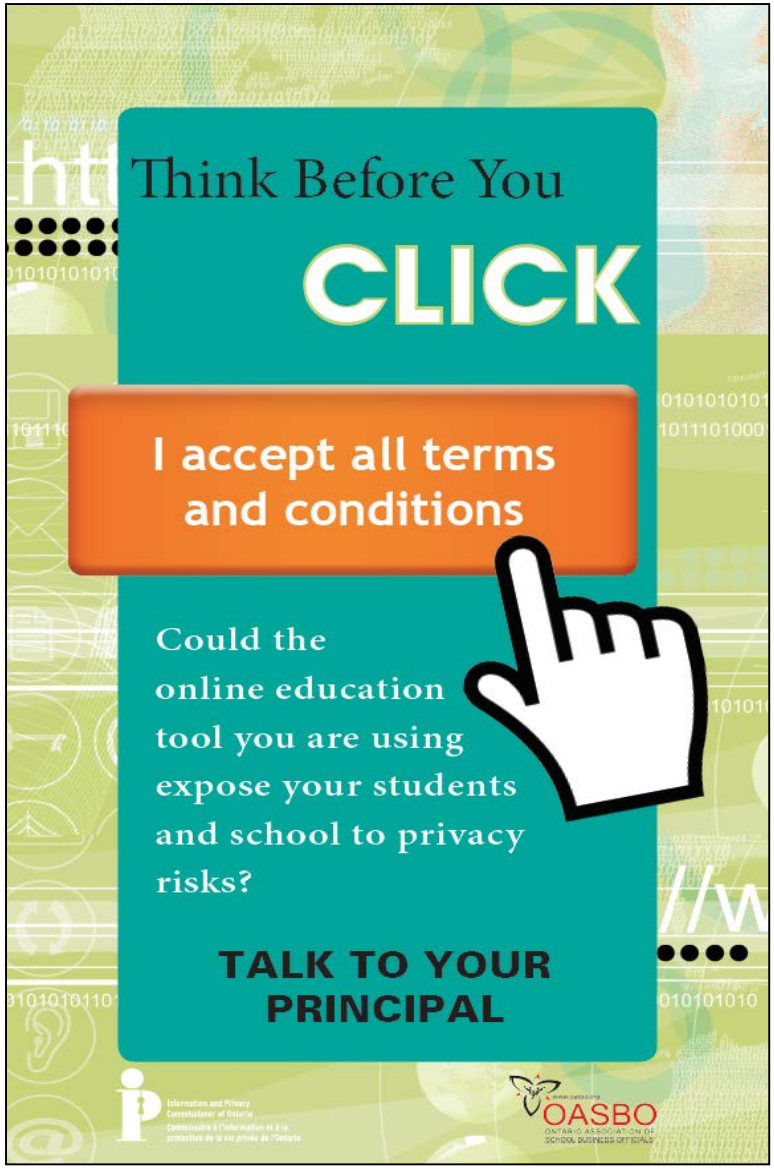


Yes, You Can

- IPC collaborates with Provincial Advocate for Children and Youth on guide about privacy and children's aid societies
- dispels myths, explains privacy legislation not a barrier to sharing information about a child who may be at risk [see *CFSA*]
- aimed mainly at school, police, social services, health care staff

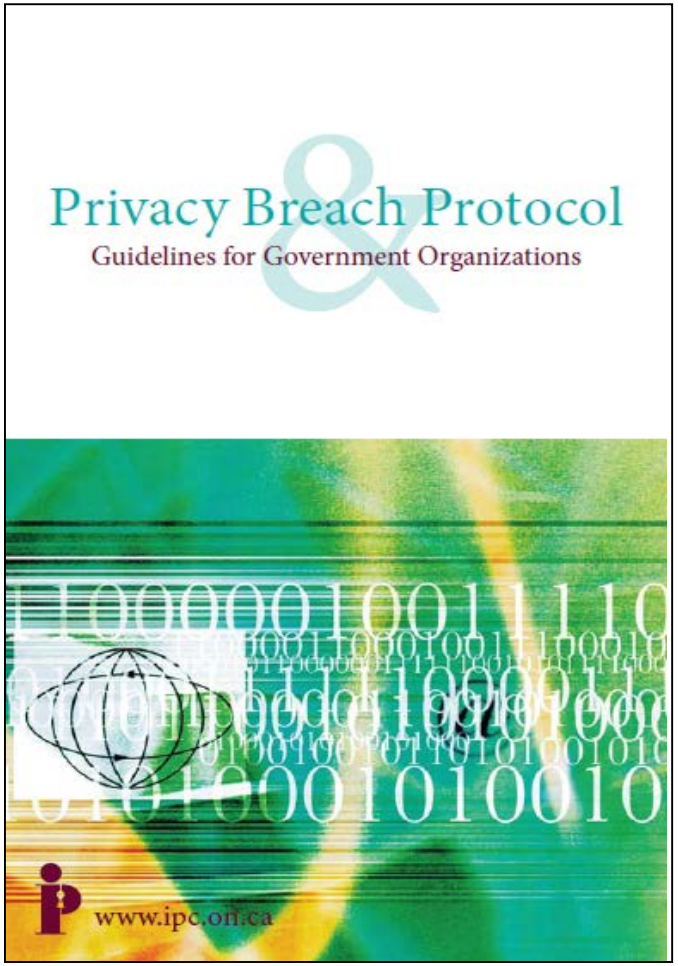


- online educational services innovative, accessible, cost little or nothing, but may pose privacy risks to students and parents
- may also impact a school board's ability to respond to students' requests for their own records
- teachers should ask their school board about services that have been approved for classroom use



Privacy Breach Protocol

- privacy breach protocol helps identify privacy risks, potential and actual breaches
- ensure training on protocol
- ensure staff know their responsibilities when a breach occurs



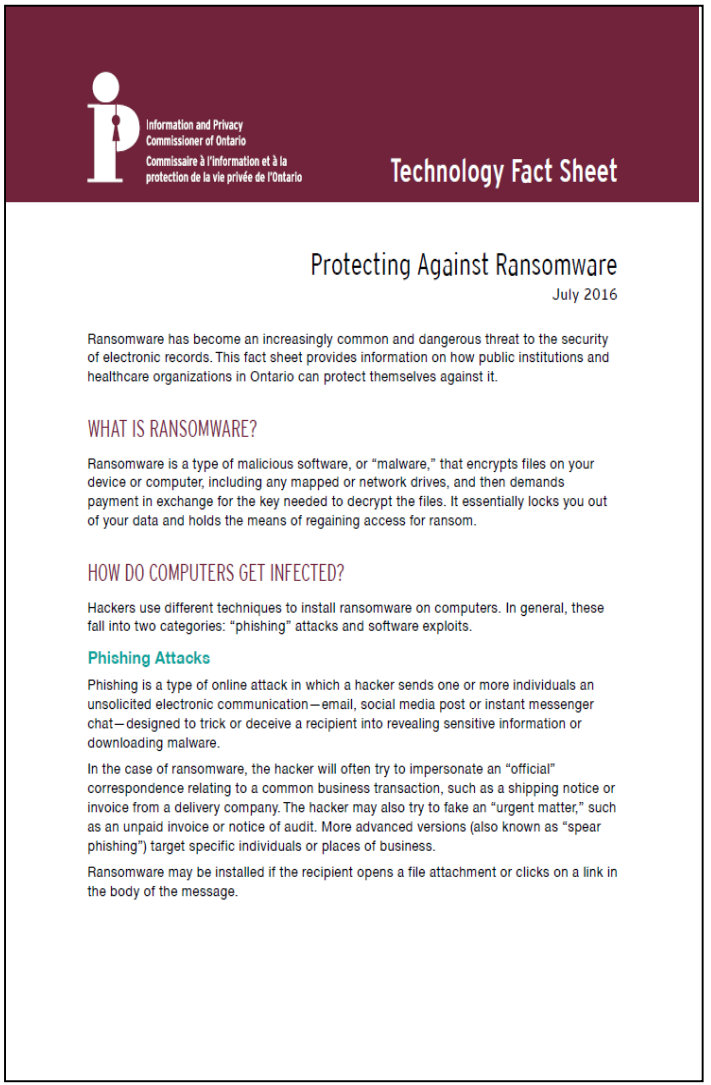
Ransomware

How Do Computers Get Infected?

- phishing attacks
- software exploits

How to Protect Your Organization

- employee training
- back up data
- antivirus software
- update software
- quarantine suspicious emails
- minimize user privileges
- limit active content
- simulate attacks



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

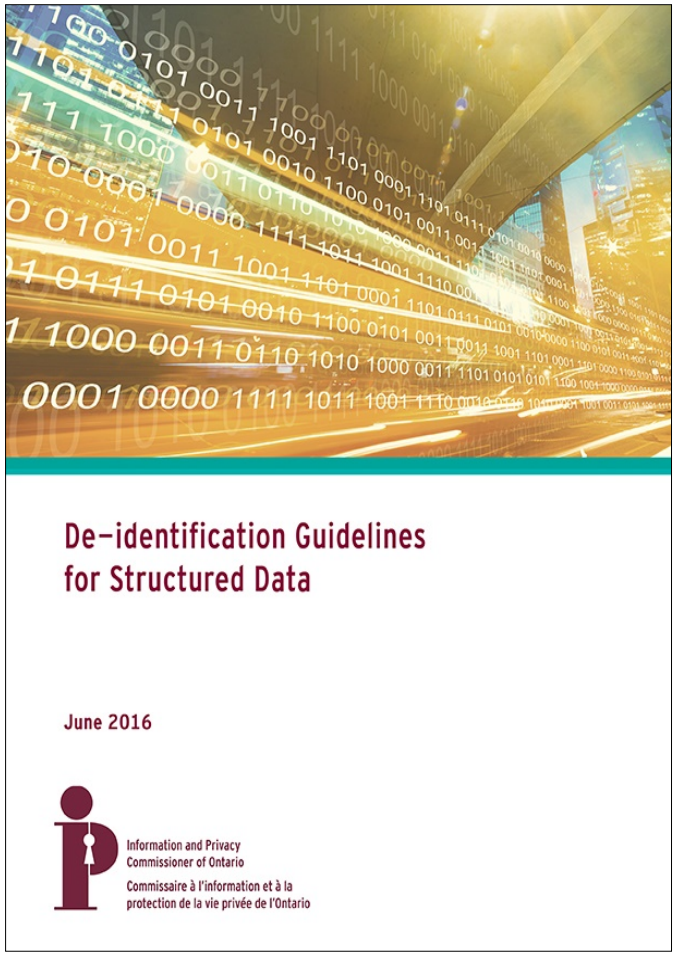
Phishing is a type of online attack in which a hacker sends one or more individuals an unsolicited electronic communication—email, social media post or instant messenger chat—designed to trick or deceive a recipient into revealing sensitive information or downloading malware.

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.

De-identification Guidelines for Structured Data

- De-identification: process of removing PI from a record or data set
- 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*



Big Data Fact Sheet

- released for Data Privacy Day (Jan 28)
- to help public understand what it is, impacts on individual privacy
- key issues:
  - proportionality
  - accuracy of results
  - bias in data sets
  - individual rights

JANUARY 2017

PRIVACY FACT SHEET

Big Data and Your Privacy Rights

New tools for combining and analyzing information have made it possible for researchers to uncover hidden patterns and connections in large data sets that would have previously been unknown. Collectively, these large data sets and the analytical tools and practices used to identify trends are known as 'big data.' While private sector companies often use big data analyses to support marketing and product development, public organizations are attracted to it as a way to improve policy and program development and ensure it is supported by better evidence.

This fact sheet has been developed to help members of the public understand what big data is, and how it can have an impact on an individual's privacy.

Big data has the potential to provide governments with greater insights into the quality and effectiveness of services and programs such as healthcare, social services, public safety and transportation. However, it also raises concerns regarding privacy and the protection of individuals' personal information.

The Office of the Information and Privacy Commissioner of Ontario (IPC) is responsible for oversight of the ***Freedom of Information and Protection of Privacy Act***, the ***Municipal Freedom of Information and Protection of Privacy Act*** and the ***Personal Health Information Protection Act***. Organizations governed by these acts, such as government ministries, municipalities, police services, health care providers and school boards, must comply with these acts when collecting, using and disclosing personal information.

This fact sheet has been developed to help members of the public understand what big data is, and how it can have an impact on an individual's privacy.

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

Coming Soon: Big Data Guidelines

- spring 2017
- for institutions, key points to consider, best practices when conducting big data projects involving personal information
  - data linking protocols
  - ethics review boards
  - public notification
  - profiling

Privacy Day Symposium
January 26, 2017

Government and Big Data: Privacy Risks and Solutions

- key issues:
  - benefits and risks of big data analytics
  - potential for bias
  - appropriate safeguards

- Guest panelists:
  - Patricia Kosseim, Senior GC, Privacy Commissioner of Canada
  - Samantha Liscio, Senior Vice President, eHealth Ontario
  - Jonathan Obar, Assistant Professor, York University
  - John Roberts, Chief Privacy Officer and Archivist of Ontario

- watch webcast at ipc.on.ca