

Investigating Privacy Lessons

Ken Anderson

Assistant Commissioner (Privacy)

Ontario

Osgoode Hall Law School

April 9, 2010

Who We Are



Commissioner Ann Cavoukian, Ph.D.

- appointed by Ontario legislature
- independent from government
- oversees 3 privacy & access to information laws

Mandated to:

- investigate privacy complaints
- resolve appeals from refusals to provide access to information
- ensure organizations comply with access and privacy provisions of the *Acts*
- educate public about Ontario's access and privacy laws
- conduct research on access and privacy issues, provide advice and comment on proposed government legislation & programs.

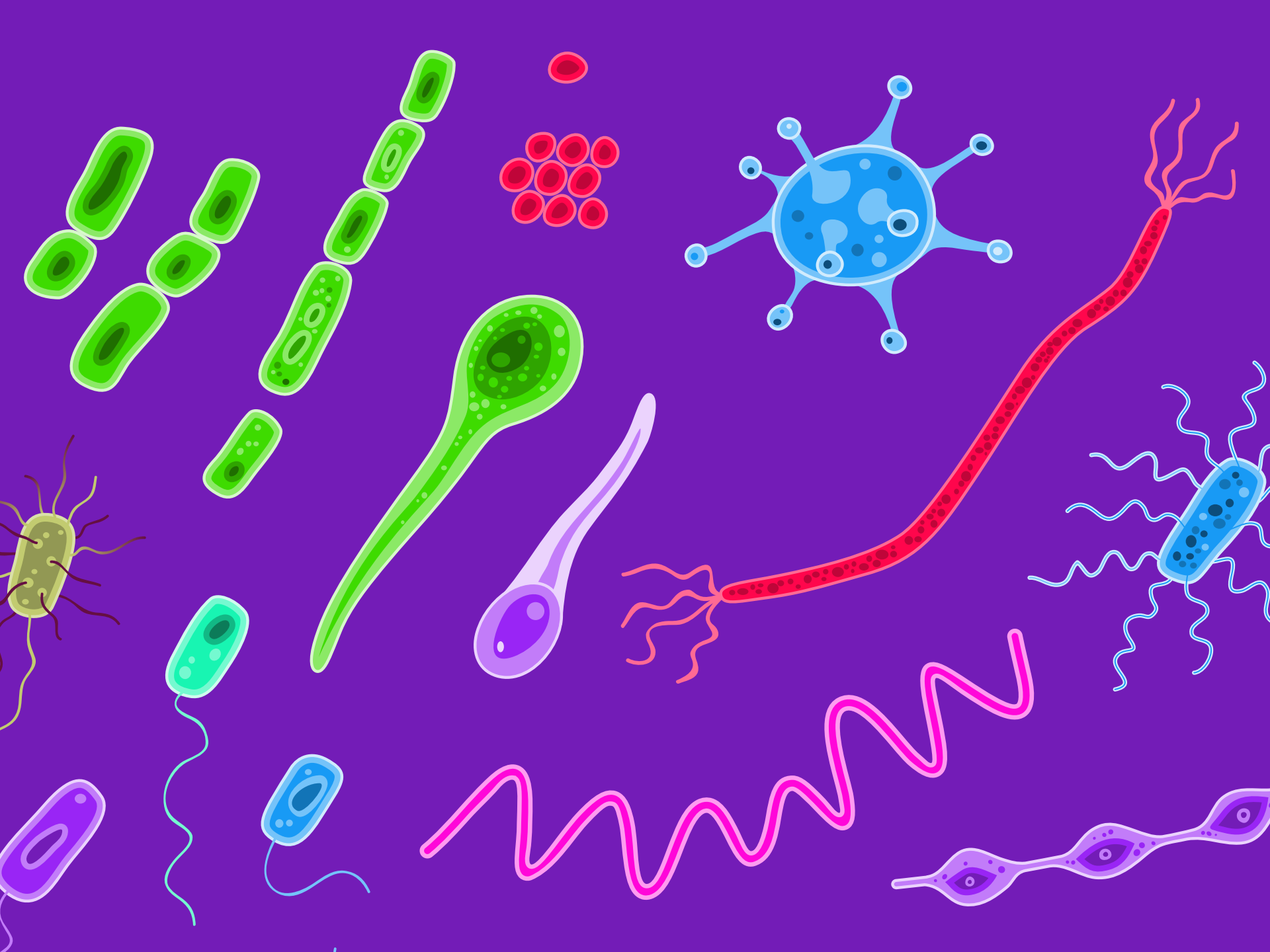


Presentation Outline

- 1. Developing a health program*
- 2. Oops*
- 3. Investigating*
- 4. Findings*
- 5. Responses*
- 6. Next...*

Developing a health program













16

17

!Tons
mk

23

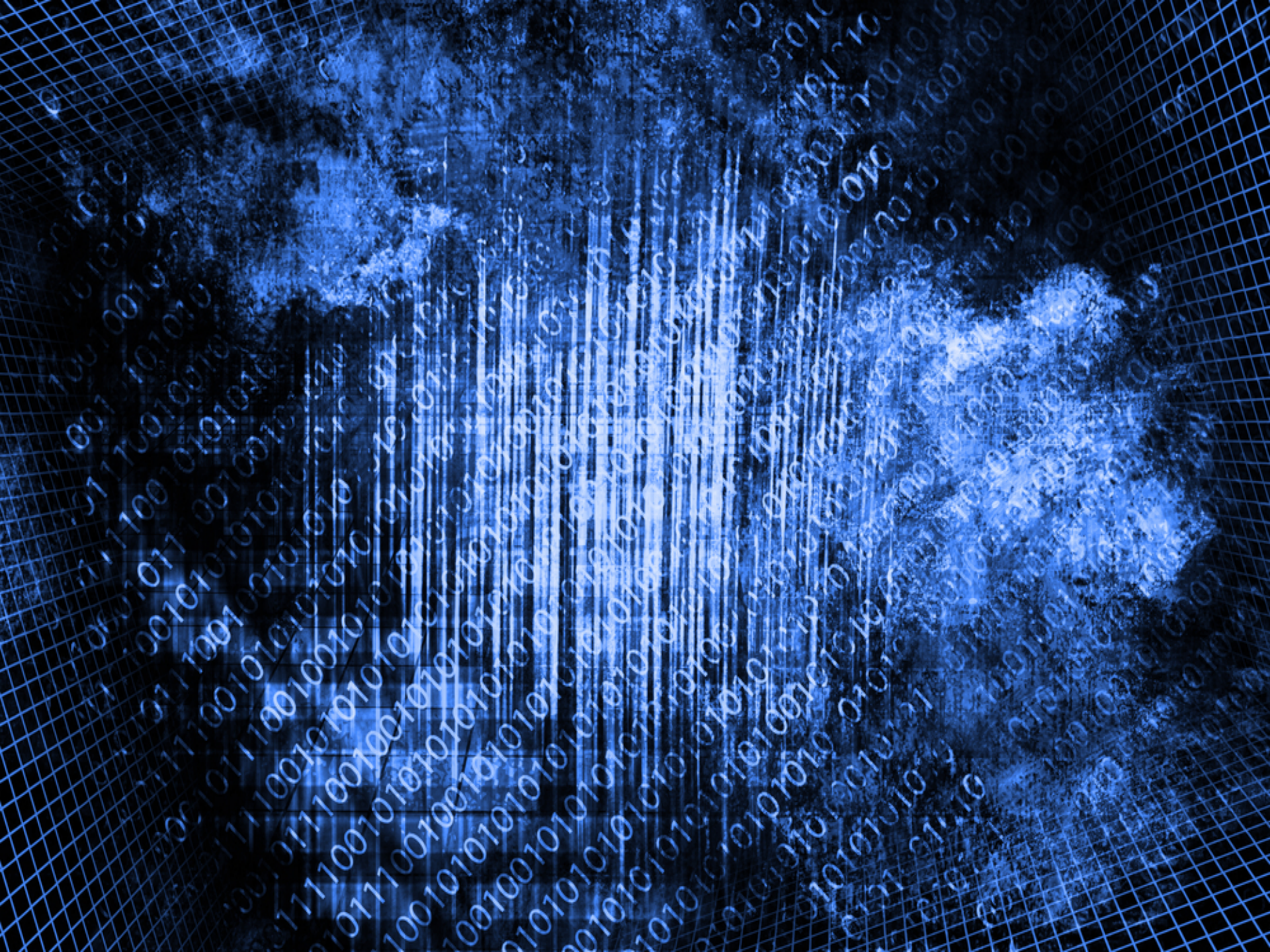
24



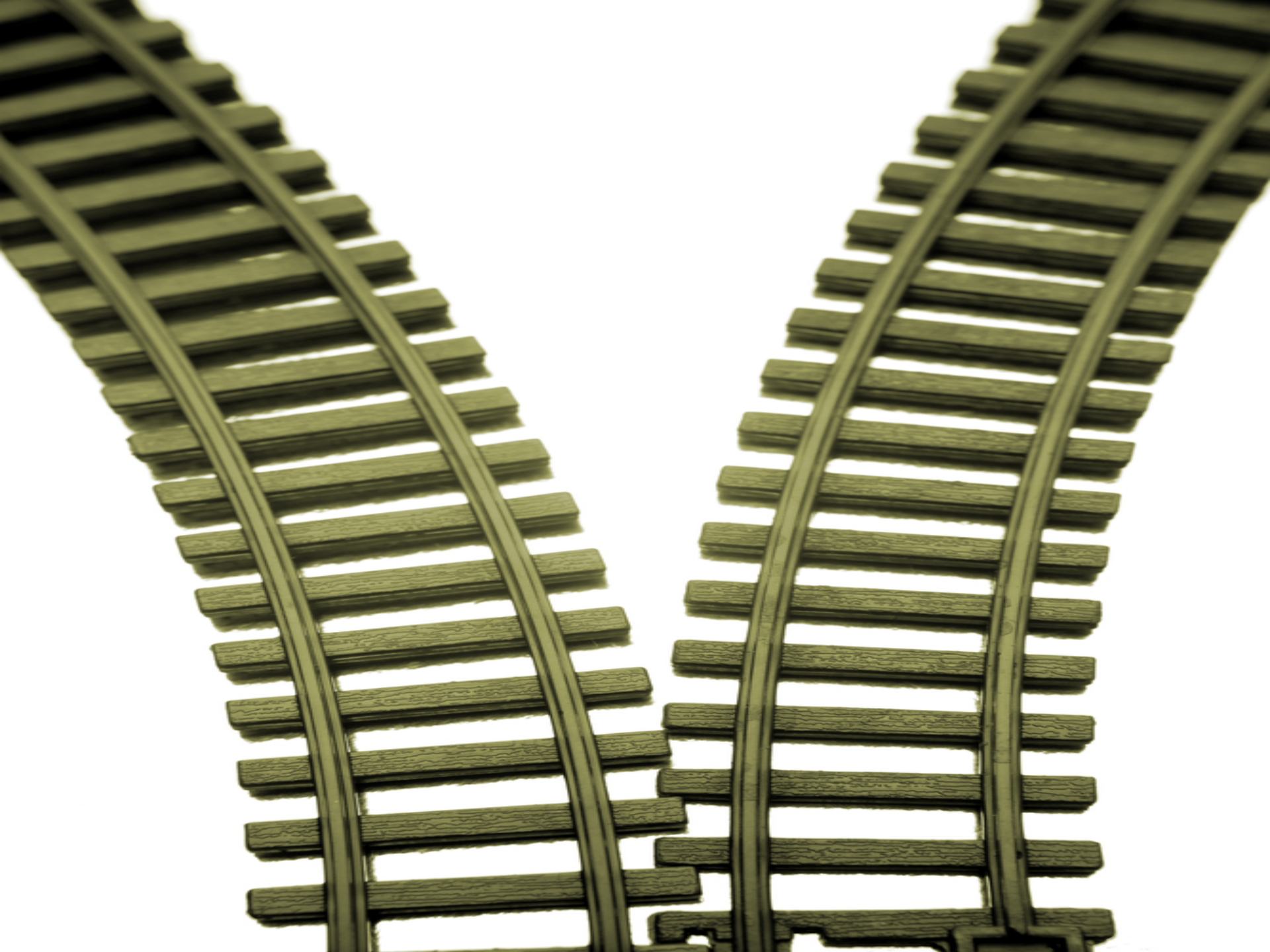








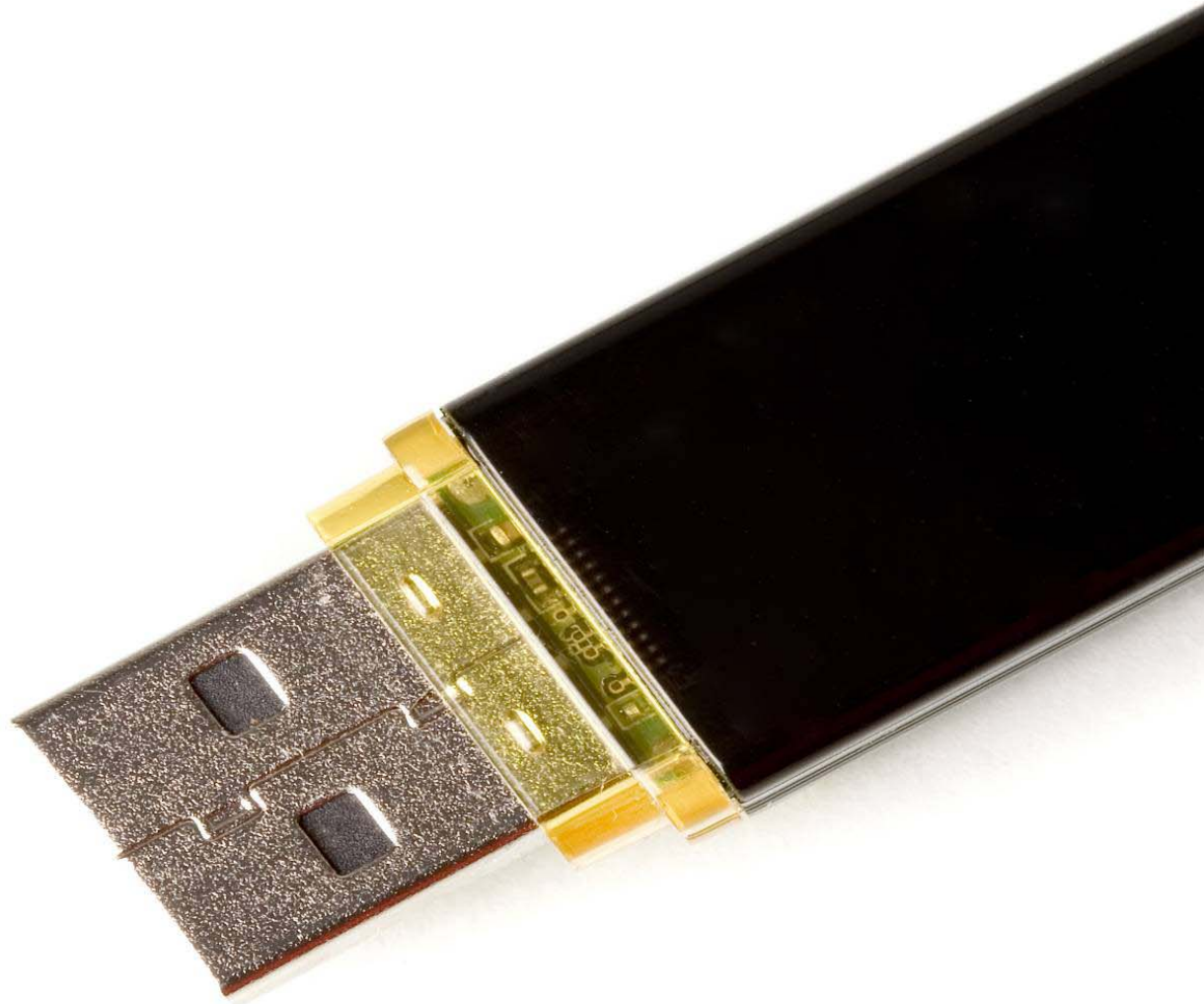
Oops!





CONNECT









Immediate Actions Taken

The Medical Officer of Health:

- Ceased collecting personal health information on mobile devices;
- Amended relevant security policies to require all mobile devices to be encrypted and to provide direction on the measures to be implemented to securely retain records of personal health information on such mobile devices;

The Assistant Deputy Minister, Public Health Division:

- Issued a memorandum reminding medical officers of health to ensure personal health information is protected against theft, loss and unauthorized use or disclosure and that records are protected against unauthorized copying, modification or disposal;

The Chief Medical Officer of Health:

- Issued a memorandum urging all medical officers of health to cease retaining or transferring personal health information on mobile devices unless strongly encrypted.

Investigating



A magnifying glass with a black frame is positioned over a document. The document has a light beige, textured background. The word "INVESTIGATION" is written in a bold, black, serif font across the center of the magnifying glass's lens. The background of the entire image is a dark, wood-grain pattern.

INVESTIGATION



Applicable Statutory Provisions

– Information Practices and Training

- A health information custodian must have and comply with information practices that meet the requirements of the *Act* (section 10);
- A health information custodian that is a natural person may designate or fulfill the role of a contact person who is, among other things, responsible for facilitating compliance with the *Act* and ensuring that agents are appropriately informed of their duties under the *Act* (section 15).

Applicable Statutory Provisions

– Security

- A health information custodian must take steps that reasonable in the circumstances to ensure that personal health information is protected against theft, loss and unauthorized use or disclosure (section 12(1));
- A health information custodian must notify individuals at the first reasonable opportunity if their personal health information is stolen, lost, or accessed by unauthorized persons (section 12(2));
- A health information custodian must ensure that records of personal health information are retained, transferred and disposed of in a secure manner (section 13).

Applicable Statutory Provisions

– Limitations on Collection

- A health information custodian shall not *collect*, use or disclose more personal health information than is reasonably necessary to meet the purpose (section 30(2)).





PHIPA ORDER No. 7 (H-007)



Findings

Order Provisions

The Medical Officer of Health was ordered to:

- Revise its information practices and implement procedures to ensure personal health information, including that retained on mobile devices, is safeguarded and strongly encrypted;
- Cease collecting health card numbers and securely dispose of health card numbers collected;
- Cease collecting personal health information related to priority groups unless relevant to the provision of the influenza vaccine immunizations;
- Securely dispose of priority group information collected after the vaccine was made widely available and that is not relevant to the provision of the influenza vaccine immunizations;
- Provide proof of compliance by February 16, 2010.

Recommendations to the Medical Officer of Health and Region of Durham

That the Medical Officer of Health:

- Take necessary steps to inform the public about the order and how to obtain a copy;

That the Regional Municipality of Durham:

- Develop and implement a comprehensive corporate policy for mobile devices to ensure that personal information transported on such devices is strongly encrypted.

Recommendations to the Ministry of Health and Chief Medical Officer of Health

That the Ministry of Health and Long-Term Care and the Chief Medical Officer of Health:

- Request each public health unit to conduct a review of its practices and procedures to ensure personal health information retained on mobile devices is strongly encrypted;
- Request each medical officer of health to provide an attestation that unencrypted personal health information is not being transported on mobile devices;
- Audit a representative sample of public health units to verify the attestation;
- Develop training materials to ensure staff of public health units are aware of the need for proper safeguards when retaining personal health information on mobile devices.

What Does Ontario's Information and Privacy Commissioner Mean By Strong Encryption?

- Does not refer to a particular technical or design specification;
- Refers to the high degree of confidence that a health information custodian must have that plaintext personal health information will not be disclosed to unauthorized persons;
- Strong encryption means that the method and choice of encryption should be:
 - Commensurate with and responsive to all threats and risks identified;
 - Consistent with evolving industry standards and practices;
 - Thoroughly integrated into operations and supported by in-depth security policies, procedures and practices;
 - Subject to ongoing security reviews and updates.



Responses

Actions Taken By Medical Officer of Health: General Information Practices and Training

- Developed a privacy and security framework to provide the foundation for a privacy program;
- Drafted an overarching privacy and security policy and reviewed the supporting privacy and information security policies which will be revised and finalized by May 2010;
- In the process of retaining an agent to implement and manage the privacy program;
- Agents in the information technology department required to attend customized training;
- In the process of amending the privacy and security training program for all agents.

Actions Taken By Medical Officer of Health: Encryption of Mobile Devices

- Developed and implemented policies and procedures that prohibit the use of:
 - Mobile computing devices to retain personal health information unless strongly encrypted;
 - Mobile media to retain personal health information unless the data is strongly encrypted;
- Ensured that all mobile computing devices were strongly encrypted and executed written attestations detailing the method of encryption employed.

Actions Taken By Medical Officer of Health: Cease Collection and Secure Disposal


- Ceased collecting health card numbers and information relating to priority groups that is not relevant to the provision of the influenza vaccine immunizations;
- Executed written attestations confirming the cessation of collection;
- Identified and securely disposed of previously collected health card numbers and priority group information that was not relevant to the provision of health care;
- Executed written attestations confirming the procedure used in securely disposing of the health card numbers and priority group information identified above;
- An audit was conducted of a certain percentage of records of personal health information to ensure that the above noted information was deleted.

Other Actions Taken

- Medical Officer of Health informed the public about the order through notices in six local newspapers and on the website;
- Regional Municipality of Durham developed and implemented a regional encryption policy;
- Ministry of Health and Long-Term Care hosted the “Public Health Law Day” on February 24, 2010, which included a one-hour plenary session on “Privacy Statutes and Associated Practice Considerations,” where a representative of the IPC spoke.

Next...





PbD

www.privacybydesign.ca



SmartPrivacy

www.smartprivacy.ca



Privacy by Design – “The sine qua non”

LAW - REGULATION & INDEPENDENT OVERSIGHT

EDUCATION & AWARENESS

ACCOUNTABILITY & TRANSPARENCY

AUDIT & CONTROL

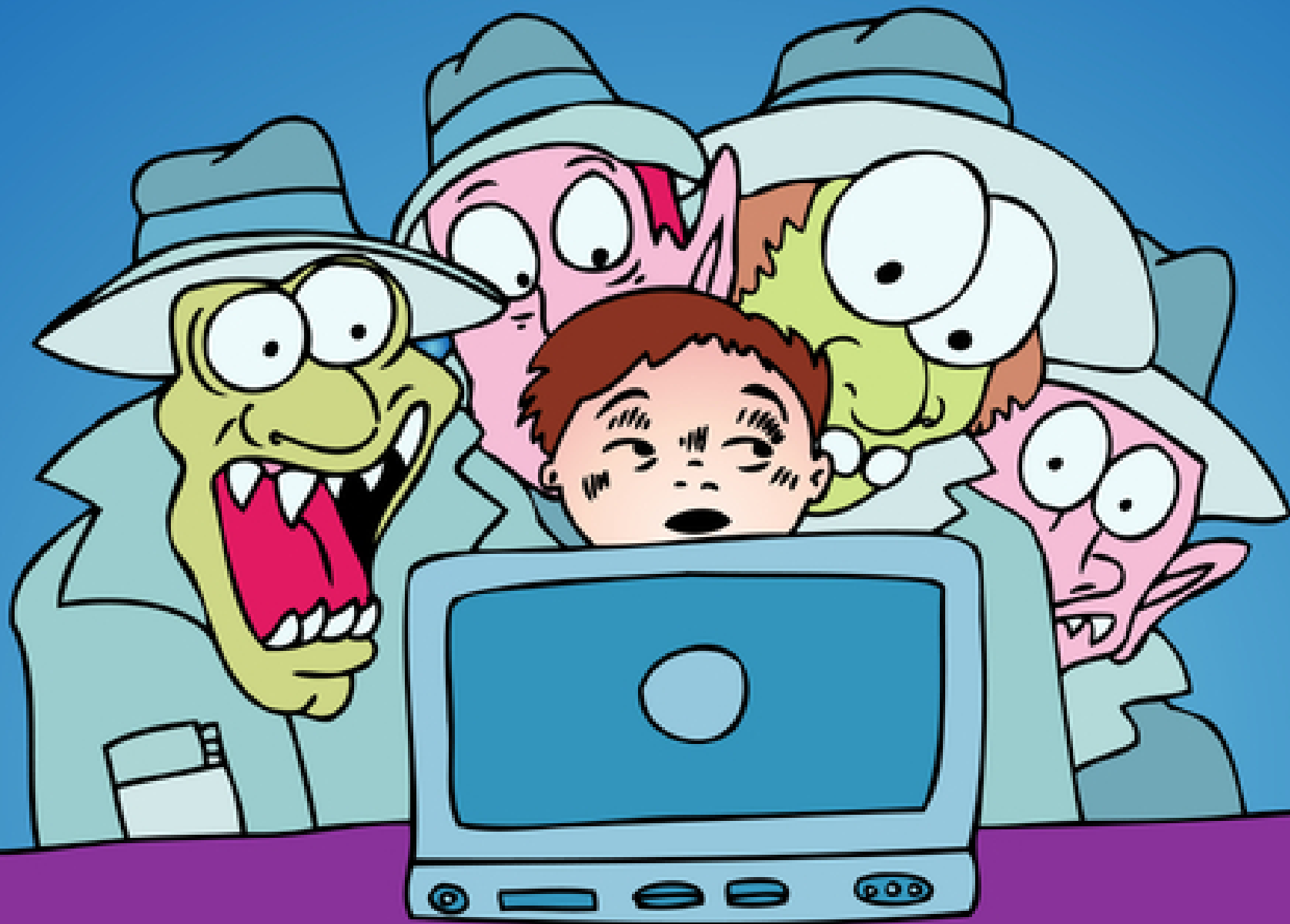
MARKET FORCES

Data Security

Fair Information Practices







How to Contact Us

Ken Anderson – Assistant Commissioner (Privacy)

IPC Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada

M4W 1A8

Phone: (416) 326-3333/ 1-800-387-0073

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca