A Glimpse at Privacy in the Past Year

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner
Ontario

Ministry of Government Services
Access and Privacy Workshop 2008
October 7, 2008

A Glimpse at Privacy in the Past Year

Three Significant Events

Three year review of *Personal Health Information Protection Act* (PHIPA);

- *PHIPA* is working well and does not require significant amendment;

Google/YouTube vs. Viacom Inc;

- Agreement signed where Google would be allowed to anonymize user data;

Online Social Networking:

- September 4, 2008 –

  Youth Privacy Online Workshop.

2007/2008:

A Banner Year for Letters to Editor

THE GLOBE AND MAIL

Privacy laws don't forbid it
The Globe And Mail
Friday, April 25, 2008
Page: A18
Section: Letter To The Editor
Byline: Ann Cavoukian

NATIONAL POST

Don't make a mockery of privacy
National Post
Thursday, Nov. 8, 2007
Page: A25
Section: Letters
Byline: Ann Cavoukian

TORONTO STAR

A blow to personal privacy
The Toronto Star
Friday, April 18, 2008
Page: AA05
Section: Letter
Byline: Ann Cavoukian

THE GLOBE AND MAIL

Privacy piracy
The Globe And Mail
Monday, June 23, 2008
Page: A14
Section: Letter To The Editor
Byline: Ann Cavoukian

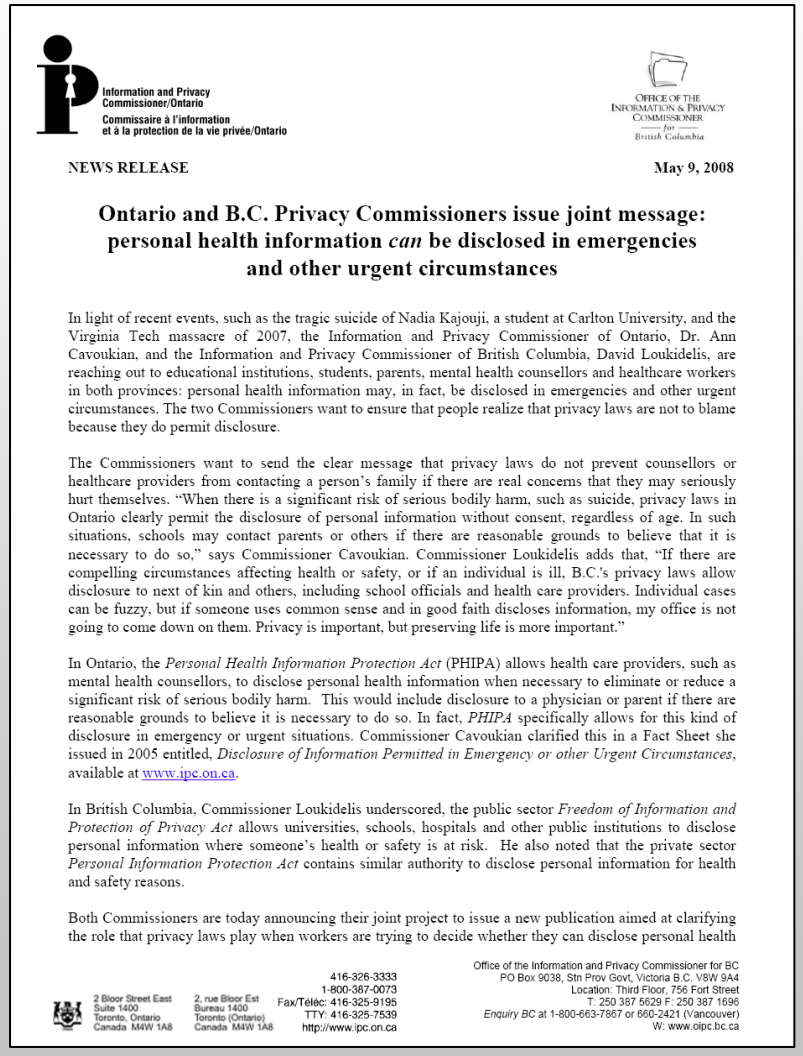
NATIONAL POST

Privacy not an absolute
National Post
Friday, April 25, 2008
Page: A13
Section: Letters
Byline: Ann Cavoukian

TORONTO STAR

Privacy laws not to blame
The Toronto Star
Thursday, April 24, 2008
Page: AA05
Section: Letter
Byline: Ann Cavoukian

Emergency Disclosures



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

Office of the Information & Privacy Commissioner for British Columbia

NEWS RELEASE

May 9, 2008

Ontario and B.C. Privacy Commissioners issue joint message: personal health information *can* be disclosed in emergencies and other urgent circumstances

In light of recent events, such as the tragic suicide of Nadia Kajouji, a student at Carlton University, and the Virginia Tech massacre of 2007, the Information and Privacy Commissioner of Ontario, Dr. Ann Cavoukian, and the Information and Privacy Commissioner of British Columbia, David Loukidelis, are reaching out to educational institutions, students, parents, mental health counsellors and healthcare workers in both provinces: personal health information may, in fact, be disclosed in emergencies and other urgent circumstances. The two Commissioners want to ensure that people realize that privacy laws are not to blame because they do permit disclosure.

The Commissioners want to send the clear message that privacy laws do not prevent counsellors or healthcare providers from contacting a person's family if there are real concerns that they may seriously hurt themselves. "When there is a significant risk of serious bodily harm, such as suicide, privacy laws in Ontario clearly permit the disclosure of personal information without consent, regardless of age. In such situations, schools may contact parents or others if there are reasonable grounds to believe that it is necessary to do so," says Commissioner Cavoukian. Commissioner Loukidelis adds that, "If there are compelling circumstances affecting health or safety, or if an individual is ill, B.C.'s privacy laws allow disclosure to next of kin and others, including school officials and health care providers. Individual cases can be fuzzy, but if someone uses common sense and in good faith discloses information, my office is not going to come down on them. Privacy is important, but preserving life is more important."

In Ontario, the *Personal Health Information Protection Act* (PHIPA) allows health care providers, such as mental health counsellors, to disclose personal health information when necessary to eliminate or reduce a significant risk of serious bodily harm. This would include disclosure to a physician or parent if there are reasonable grounds to believe it is necessary to do so. In fact, *PHIPA* specifically allows for this kind of disclosure in emergency or urgent situations. Commissioner Cavoukian clarified this in a Fact Sheet she issued in 2005 entitled, *Disclosure of Information Permitted in Emergency or other Urgent Circumstances*, available at www.ipc.on.ca.

In British Columbia, Commissioner Loukidelis underscored, the public sector *Freedom of Information and Protection of Privacy Act* allows universities, schools, hospitals and other public institutions to disclose personal information where someone's health or safety is at risk. He also noted that the private sector *Personal Information Protection Act* contains similar authority to disclose personal information for health and safety reasons.

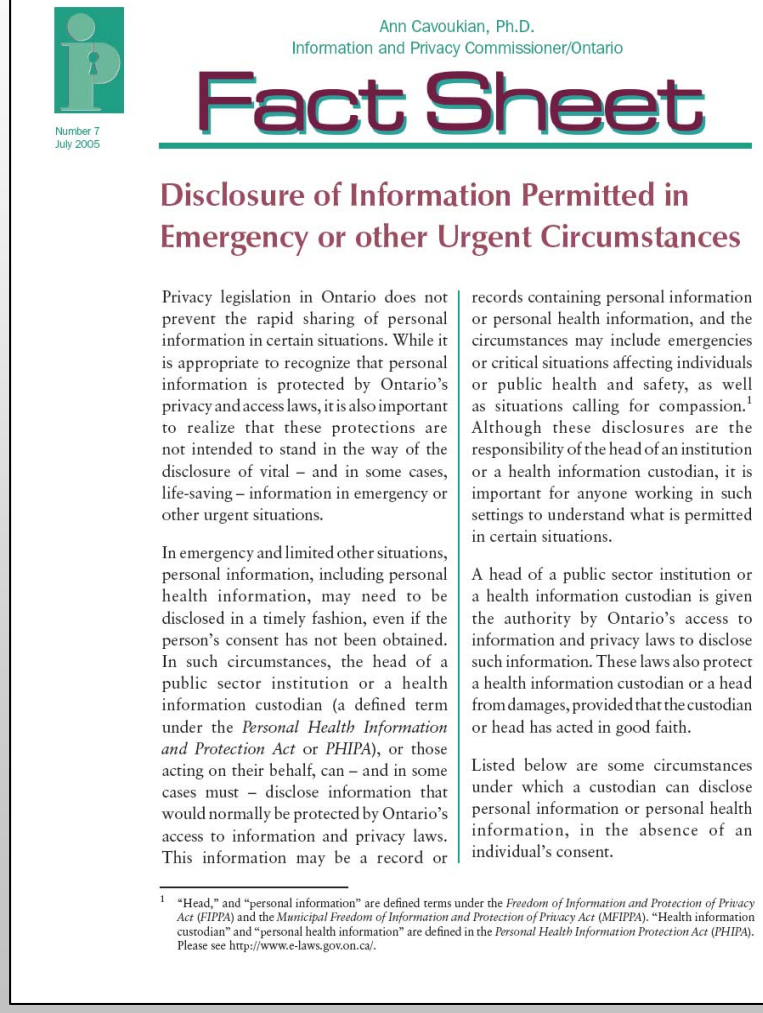
Both Commissioners are today announcing their joint project to issue a new publication aimed at clarifying the role that privacy laws play when workers are trying to decide whether they can disclose personal health

2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9195
TTY: 416-325-7539
http://www.ipc.on.ca

Office of the Information and Privacy Commissioner for BC
PO Box 9038, Stn Prov Govt, Victoria B.C. V8W 9A4
Location: Third Floor, 756 Fort Street
T: 250 387 5629 F: 250 387 1696
Enquiry BC at 1-800-663-7867 or 660-2421 (Vancouver)
W: www.oipc.bc.ca



Number 7
July 2005

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner/Ontario

Fact Sheet

Disclosure of Information Permitted in Emergency or other Urgent Circumstances

Privacy legislation in Ontario does not prevent the rapid sharing of personal information in certain situations. While it is appropriate to recognize that personal information is protected by Ontario's privacy and access laws, it is also important to realize that these protections are not intended to stand in the way of the disclosure of vital – and in some cases, life-saving – information in emergency or other urgent situations.

In emergency and limited other situations, personal information, including personal health information, may need to be disclosed in a timely fashion, even if the person's consent has not been obtained. In such circumstances, the head of a public sector institution or a health information custodian (a defined term under the *Personal Health Information and Protection Act* or *PHIPA*), or those acting on their behalf, can – and in some cases must – disclose information that would normally be protected by Ontario's access to information and privacy laws. This information may be a record or records containing personal information or personal health information, and the circumstances may include emergencies or critical situations affecting individuals or public health and safety, as well as situations calling for compassion.[1] Although these disclosures are the responsibility of the head of an institution or a health information custodian, it is important for anyone working in such settings to understand what is permitted in certain situations.

A head of a public sector institution or a health information custodian is given the authority by Ontario's access to information and privacy laws to disclose such information. These laws also protect a health information custodian or a head from damages, provided that the custodian or head has acted in good faith.

Listed below are some circumstances under which a custodian can disclose personal information or personal health information, in the absence of an individual's consent.

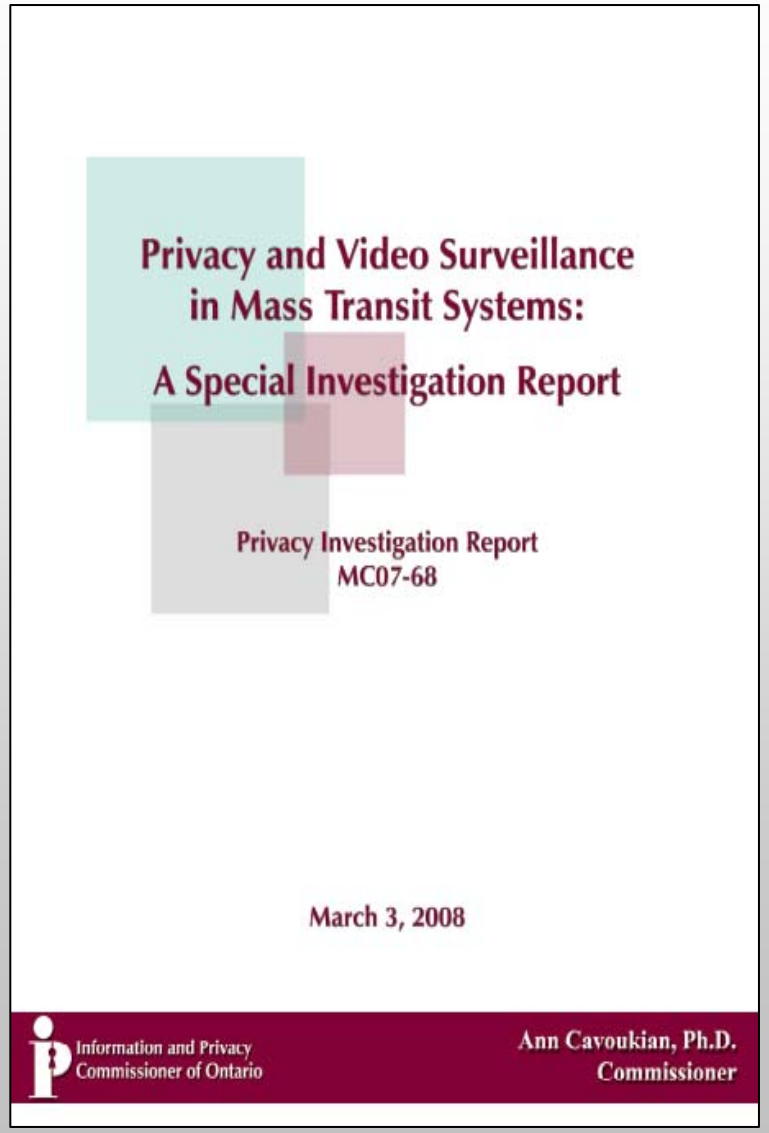
[1] "Head," and "personal information" are defined terms under the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) and the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*). "Health information custodian" and "personal health information" are defined in the *Personal Health Information Protection Act* (*PHIPA*). Please see http://www.e-laws.gov.on.ca/.

www.ipc.on.ca/images/Resources/up-3fact_07_e.pdf

New Perspectives

TTC Surveillance Cameras

- In March 2008, I ruled that Toronto's Mass Transit System's use of video surveillance cameras was in compliance with Ontario's privacy law.
- However, I called upon the TTC to undertake a number of specific measures to enhance privacy:
  - Personal information will only be collected for legitimate, limited and specific purposes;
  - Collection will be limited to the minimum necessary and **only retained up to 72 hours;**
  - A comprehensive audit of the video surveillance system must be conducted by an independent third party using the GAPP (Generally Accepted Privacy Principles) framework.



www.ipc.on.ca/images/Findings/mc07-68-ttc.pdf

TTC Report:
What the Experts are Saying

"The report is a valuable step forward toward ensuring that video surveillance be carried out in ways that ensure that privacy is protected and that oversight exists."

— Professor Daniel J. Solove, Associate Professor of Law,
George Washington University Law School

"While I understand your report is specifically addressing only the Toronto Transit Commission, it will be invaluable to municipalities throughout the world which are facing similar vexing questions about the proper use and management of video surveillance technologies. Your recommendations provide a principled yet workable model for how to protect individuals' legal and moral right to privacy while also advancing the public's interest in safe, efficient and affordable infrastructure."

— Professor Fred Cate, Distinguished Professor of Law and
Director, Center for Applied Cybersecurity Research

TTC Report: What the Experts are Saying (Cont'd)

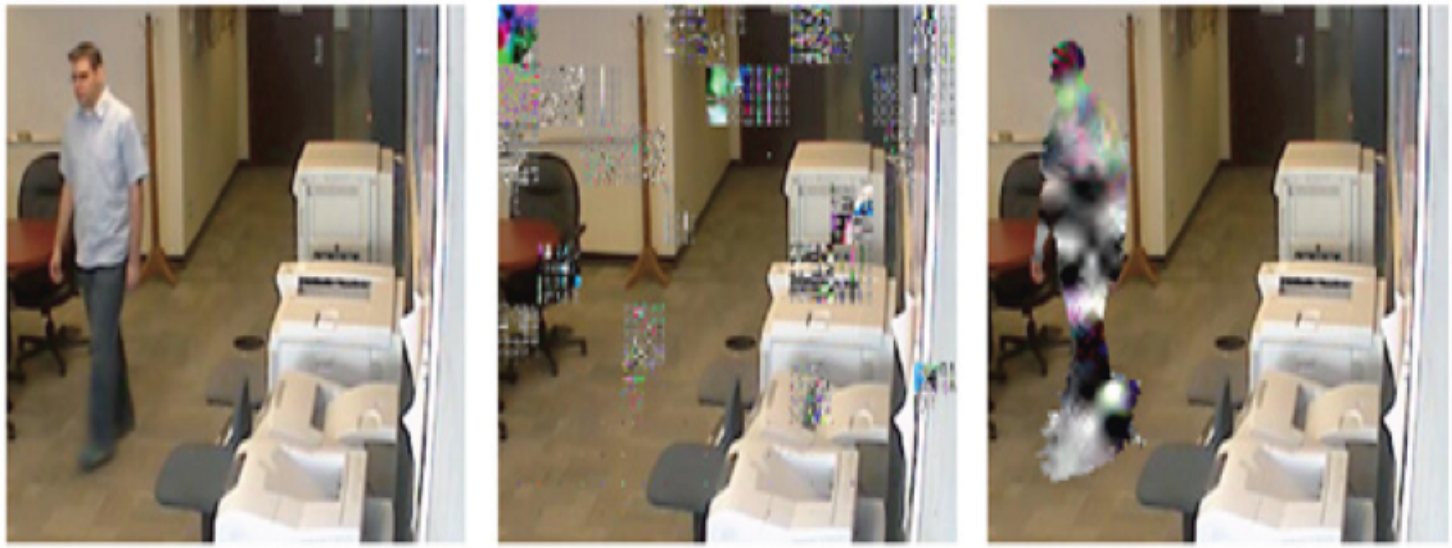
"It sets the bench mark for informed discussion of CCTV in mass transit systems … It provides a roadmap for the most privacy protective approach to CCTV. It offers potential technological solutions that can further enhance privacy with CCTV imagery. It presents specific recommendations and a requirement for an independent third-party audit (this is the Commissioner flexing her muscles). Finally, it demonstrates that … good system design, vigilant oversight, and a commitment to privacy values can result in 'positive-sum' models as Commissioner Cavoukian describes them."

— Murray Long, Editor and Publisher,
PrivacyScan

CCTV Cameras: *Innovative Privacy-Enhancing Approach to Video Surveillance*

- At the University of Toronto, Professor Kostas Plataniotis and Karl Martin have developed a privacy-enhancing approach to video surveillance cameras;
- Their work, as described in *Privacy Protected Surveillance Using Secure Visual Object Coding*, uses cryptographic techniques to secure a private object (a face/image), so that it may only be viewed by designated persons;
- Objects of interest (e.g. a face or body) are stored as completely separate entities from the background surveillance frame, and strongly encrypted.

Innovative Privacy-Enhancing "Transformative" Approach

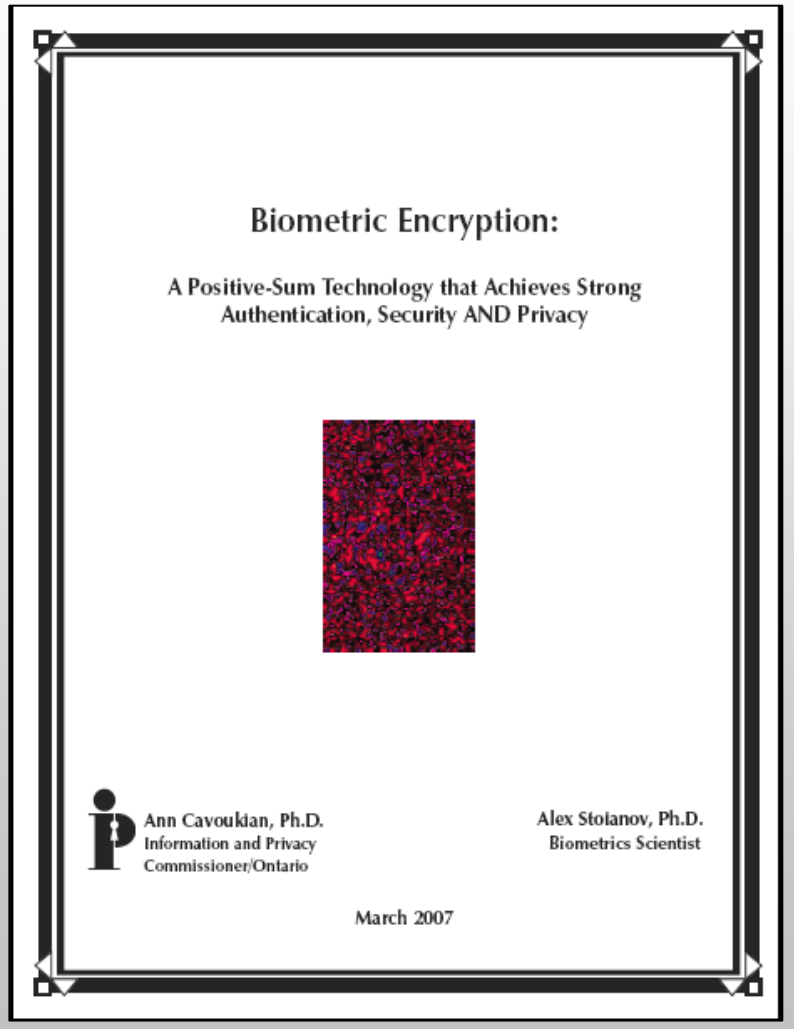


(a) (b) (c)

Figure (a): original content stream; Figure (b): both shape and texture have been encrypted and despite attempts to hack into this with an incorrect key, the objects of interest could not be decrypted; Figure (c): example where only the texture of the whole body (or only a face for example) is encrypted.

Biometrics Transformed: *IPC Biometrics Paper*

- This paper discusses the privacy-enhanced uses of biometrics, with a particular focus on the privacy and security advantages of Biometric Encryption (BE) – the merits of the BE approach to verifying identity, protecting privacy, and ensuring security;
- The central message is that BE can help to overcome the prevailing "zero-sum" mentality by adding privacy to identification and information systems, resulting in a positive-sum, scenario for all stakeholders.



www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf

Privacy by Design: "Build It In"

- Build in privacy – up front, into the design specifications; into the architecture; if possible embed privacy right into the technology used – ***bake it in***;
- Assess the risks to privacy: conduct a privacy impact assessment; follow up with annual privacy audits;
- Data minimization is key: minimize the routine collection and use of personally identifiable information – use encrypted or coded information whenever possible;
- Use privacy-enhancing technologies (PETs) where possible: give people maximum control over their own data.

From PETs to Trans Tech

Transformative Technologies

Surveillance Technology + Positive-Sum Paradigm + Privacy-Enhancing Technology = Transformative Technology

Common characteristics of Transformative Technologies:

- Minimize the unnecessary collection, disclosure, use and retention of personal data;
- Empower individuals to participate in the management of their own personal data;
- Enhance the security of personal data, if collected/used;
- Promote public confidence and trust in personal data governance structures;
- Promote/facilitate the commercialization and adoption of these technologies.

Pragmatism

Radical
Pragmatism

Radical

Radical

(/raedikel/ adj, & n.) — adj.

2) **far-reaching … thorough.**

— Concise Oxford Dictionary, Eighth Edition, 1990.

Radical Privacy Pragmatism

Radical = far-reaching … thorough;

Pragmatism ≠ status quo;

Radical Pragmatism (in the area of privacy)
is the embodiment of a positive-sum paradigm,
involving a practical approach,
invoking the need for
Transformative Technologies;

Talk – Action = Zero

Conclusions

- Do NOT use privacy as a roadblock for withholding information when you should and can disclose it;
- Think "Positive-Sum," not "Zero-Sum;"
- Make access to information **and** privacy fundamental business considerations for the government of Ontario;
- Privacy by Design – "Build it In:" From PETs to Transformative Technologies;
- Access to Information is alive and well – **Canada's "Right to Know Week."**

How to Contact Us

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario, Canada
M4W 1A8

Phone: (416) 326-3948 / 1-800-387-0073
Web: www.ipc.on.ca
E-mail: info@ipc.on.ca