Ensuring the Future of Privacy: Build It In

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

International Association of Privacy Professionals
Canadian Privacy Summit
May 1, 2009

Presentation Outline

1. *Privacy by Design*
2. *The Next Wave: From PETs to PETs Plus, … to Transformative Technologies*
3. *Privacy in the Clouds: Networked Computing*
4. *Federated-PIA and PRM*
5. *Conclusions*

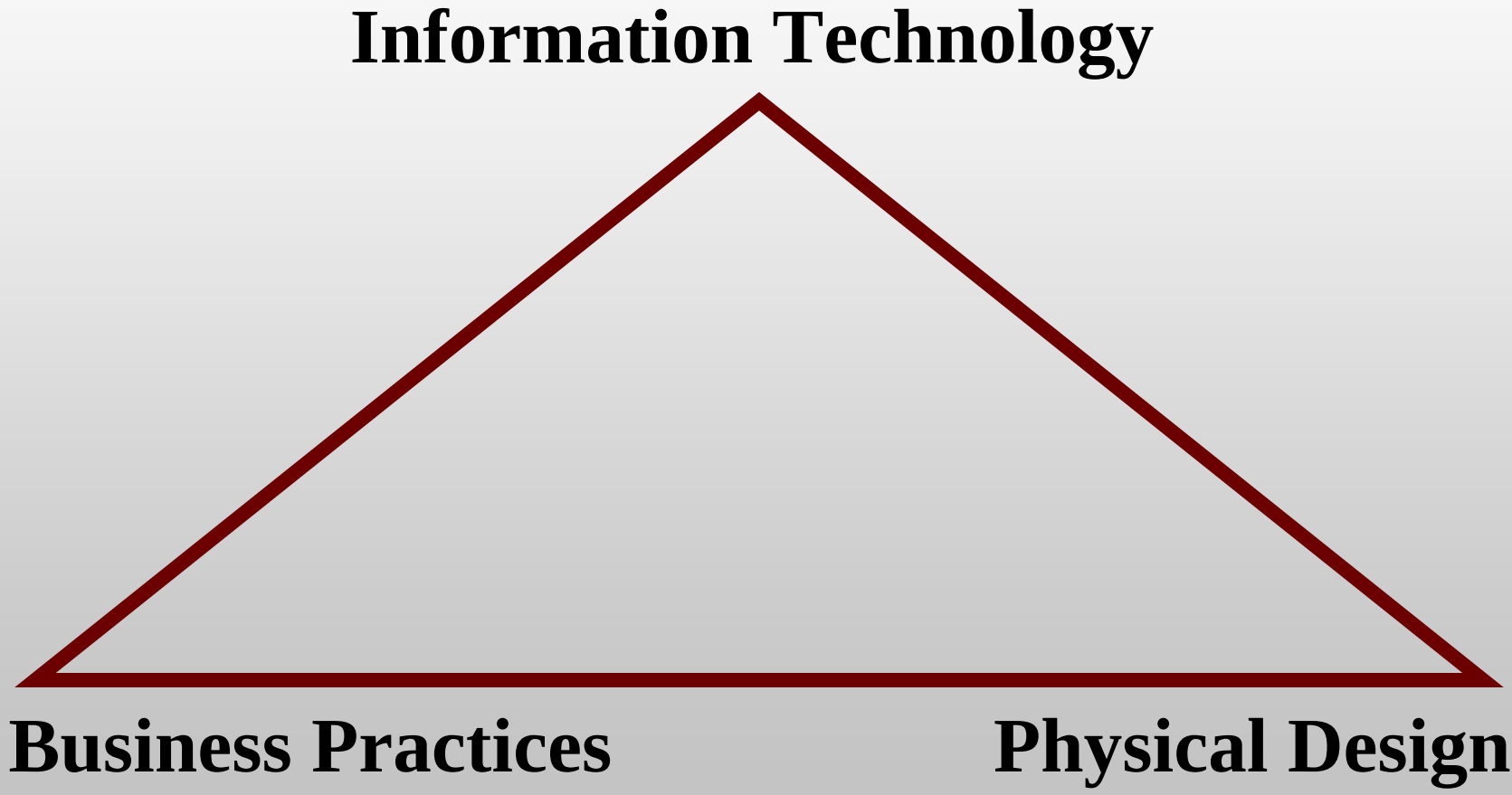
Privacy by Design


PbD

Privacy by Design: "Build It In"

- I first developed the term "Privacy by Design" in the '90s, as a response to the growing threats to online privacy that were beginning to emerge;
- "Privacy by Design" seeks to build in privacy – up front, right into the design specifications; into the architecture; thereby embedding privacy into the technology used, – ***bake it in***;
- Data minimization is key: minimize the routine collection and use of personally identifiable information – use encrypted or coded information wherever possible;
- Explore various privacy-enhancing technologies (PETs): give users maximum control over their own data.

Privacy by Design:
The Trilogy of Applications



Privacy by Design:
Focus for 2009

- **Technology** – Building privacy directly into technology, at the earliest developmental stage;
- **Business Practices** – Incorporating privacy into competitive business strategies and operations;
- **Physical Design** – Ensuring privacy in organizational and health care settings.

The Next Wave:

From PETs to PETs Plus, to Trans Tech

Background: Privacy-Enhancing Technologies *(PETs)*

- The IPC coined the concept and methodology recognized around the world today as *privacy-enhancing technologies* (PETs);
- In 1995, the IPC and the Dutch Data Protection Authority published the landmark study, *Privacy-Enhancing Technologies: The Path to Anonymity (Vols. I & II).*

  Vol. I - www.ipc.on.ca/index.asp?layid=86&fid1=329

  Vol. II - www.ipc.on.ca/images/Resources/anoni-v2.pdf

Time for a Change…

… from PETs

to …

PETs Plus

PETs *Plus*

The "*Plus*" in PETs *Plus* refers to incorporating a *positive-sum* paradigm (not zero-sum) into an existing privacy-enhancing approach

Then, take it a step further:

from PETs Plus

to

Transformative Technologies

Transformative Technologies

Privacy-Invasive Technology + Positive-Sum Paradigm + Privacy-Enhancing Technology =

<u>Transformative Technology</u>

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.

Privacy in the Clouds: Networked Computing

IPC
www.ipc.on.ca

Privacy in the Clouds

Evolution of Consumer Computing:

1. **The stand-alone PC** in which the user's software and data are stored on a single, easily protected machine, such as word processing, spreadsheets;

2. **The Web** in which most of the software a user needs is still on their own PC, but more and more of the data they need is found on the Internet, such as a Web browser;

3. **The "Cloud"** in which users rely heavily on data and software that reside externally on the Internet. Examples: using Google Apps for word-processing; virtual worlds such as Second Life that enable users to build 3D environments combining Web pages and Web applications.

   See *The Information Factories* by George Gilder, Wired magazine, October, 2006, www.wired.com/wired/archive/14.10/cloudware_pr.html

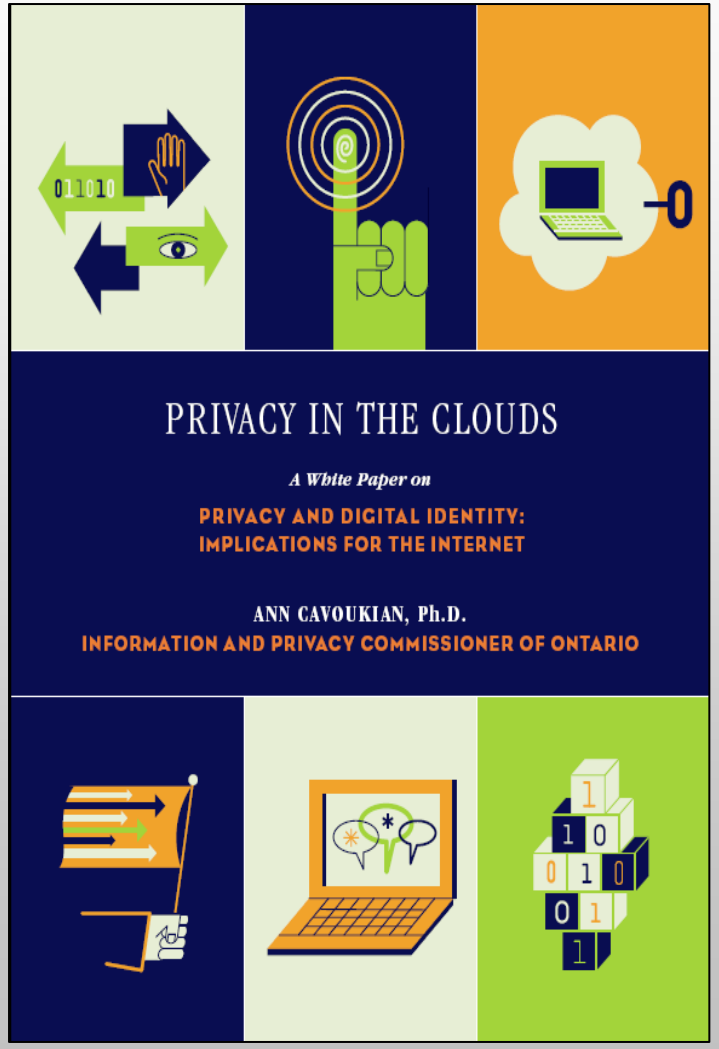
The Power and the Promise of Cloud Computing

- **Limitless flexibility**: With access to millions of different pieces of software and databases, and the ability to combine them into customized services, users are better able to find the answers they need, to share their ideas, and enjoy online games, video, and virtual worlds;
- **Better reliability and security**: Users no longer have to worry about their hard drives crashing or their laptops being stolen;
- **Enhanced collaboration**: By enabling online sharing of information and applications, the Cloud offers users new ways of working and "playing" together (think social networks);
- **Portability**: Users can access their data and tools anywhere that they can connect to the Internet;
- **Simpler devices**: With data and the software being stored in the Cloud, users no longer need a powerful computer. They can interface using a cell phone, a PDA, a personal video recorder, an online game console, their cars, or even sensors build into their clothing.

Privacy in the Clouds
(in the Web 2.0 World)

Cloud Building Blocks:

1. Open source and proprietary identity software based on open standards;
2. Federated Identity;
3. Multiple and partial identities;
4. Data-centred policies;
5. Audit tools.



www.ipc.on.ca/images/Resources%5Cprivacyintheclouds.pdf

Federated Privacy Impact Assessment (F-PIA)

Federated Privacy Impact Assessment (F-PIA)

Goals of an F-PIA:

- Provide an opportunity for members to develop and codify a Federation's privacy policies;
- Demonstrate that privacy policies, as defined by members of the Federation, will be met;
- Demonstrate that an appropriate technological architecture is in place to prevent, to the extent possible, accidental or malicious violations of privacy policies.

– 2010 –

Stay tuned for another new tool: Moving from PIA to "PRM"

- The idea for a **Privacy Risk Management (PRM)** assessment tool was first envisioned at the annual Risk and Insurance Management Society (RIMS) conference in late 2008;
- My office formed a collaborative working group with Sun Life Financial and the YMCA to develop a new tool to build a bridge between risk management and privacy concerns;
- Stay tuned – it's coming in the Spring of 2010.

Final Thought:
Educate, Educate, Educate!

- Let's not forget members of the public, the users of various programs and services;
- It's all about education – teaching users how to protect their privacy online; raising their awareness and understanding the issues.

Two Specific Areas of Engagement:

(Further to Our Mandate to Educate)

- **The Judiciary**: judicial education about online issues relating to privacy;
- **Students, professionals and the public**: how to protect your privacy online – on social networks and elsewhere.

Conclusions

- Lead with ***Privacy by Design*** – embed privacy into the design specifications of various technologies, business practices and operations;
- Take it a step further – change the paradigm from "zero-sum" to "positive-sum," where both privacy *and* security can be delivered, thereby raising the *overall* level of protection;
- When you change the paradigm, you change the mindset: you can deliver *both* privacy AND security, not the mutually exclusive "either/or;"
- The future of privacy may very well depend on embedding privacy into design – let's make it a reality;
- **Educate, educate, educate!**

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