The Future of Privacy May Rest on "Privacy by Design"

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

Computers, Freedom and Privacy Conference
Washington D.C.
June 4, 2009

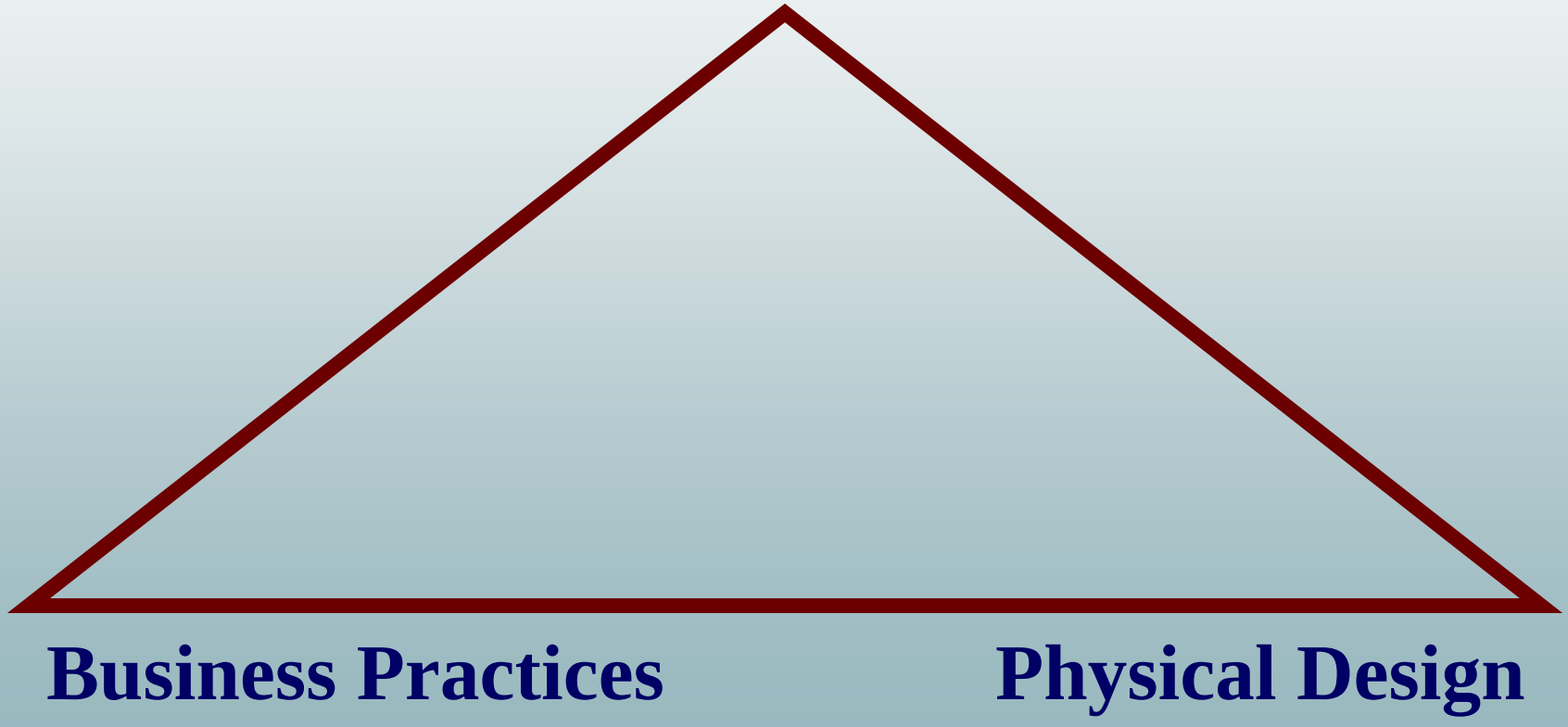

PbD
www.privacybydesign.ca

“Privacy by Design”

Privacy by Design: "Build It In"

- I first developed the concept of "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; embed 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 whenever possible;
- Use privacy-enhancing technologies (PETs) where possible: give people 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 –** Introducing privacy into organizational and health care settings.

Why We Need *Privacy by Design*

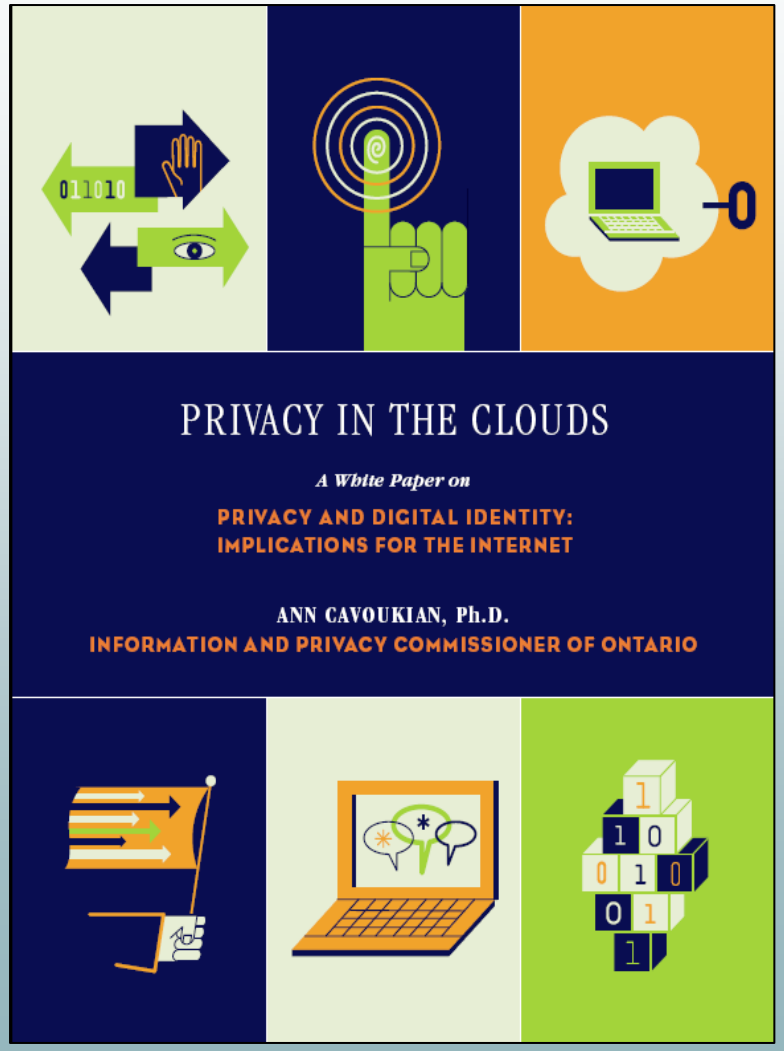
- Most privacy breaches remain undetected – as regulators, we only see the tip of the iceberg;
- The majority of privacy breaches remain unchallenged, unregulated, and unknown;
- Compliance alone, is unsustainable as a model for ensuring the future of privacy; for that, we must turn to proactive measures such as ***Privacy by Design:*** embed privacy proactively into the core of all that we do.

Privacy in the Clouds: Networked Computing

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

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.

What is Essential:

We must preserve the distinction between primary purpose vs. secondary uses

New Formulations of Collection and Use, involving …

- Fair information practices;
- Codes of practice;
- Emerging privacy laws;
- Privacy protocols …;

We must not erode the fundamental wisdom reflected in distinguishing primary purposes from secondary uses

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