SmartPrivacy:
Lead with Privacy by Design

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario

Conference Board Council of Chief Privacy Officers

September 22, 2009

Presentation Outline

1. *The Privacy Landscape*
2. *Get Smart About Privacy: SmartPrivacy*
3. *Privacy by Design –* PbD
4. *Accountable Business Practices …*
   the 2nd Rung of PbD
5. *SmartPrivacy and the Smart Grid*
6. *RFID Transformed: Add an On/Off Device*
7. *Conclusions*

The Privacy Landscape

What Privacy is Not

Privacy ≠ Security

Security *is*, however, vital to privacy

If privacy is to live well into the future, things have to change

The Future of Privacy:

Positive-Sum

NOT

Zero-Sum

We need to change the paradigm

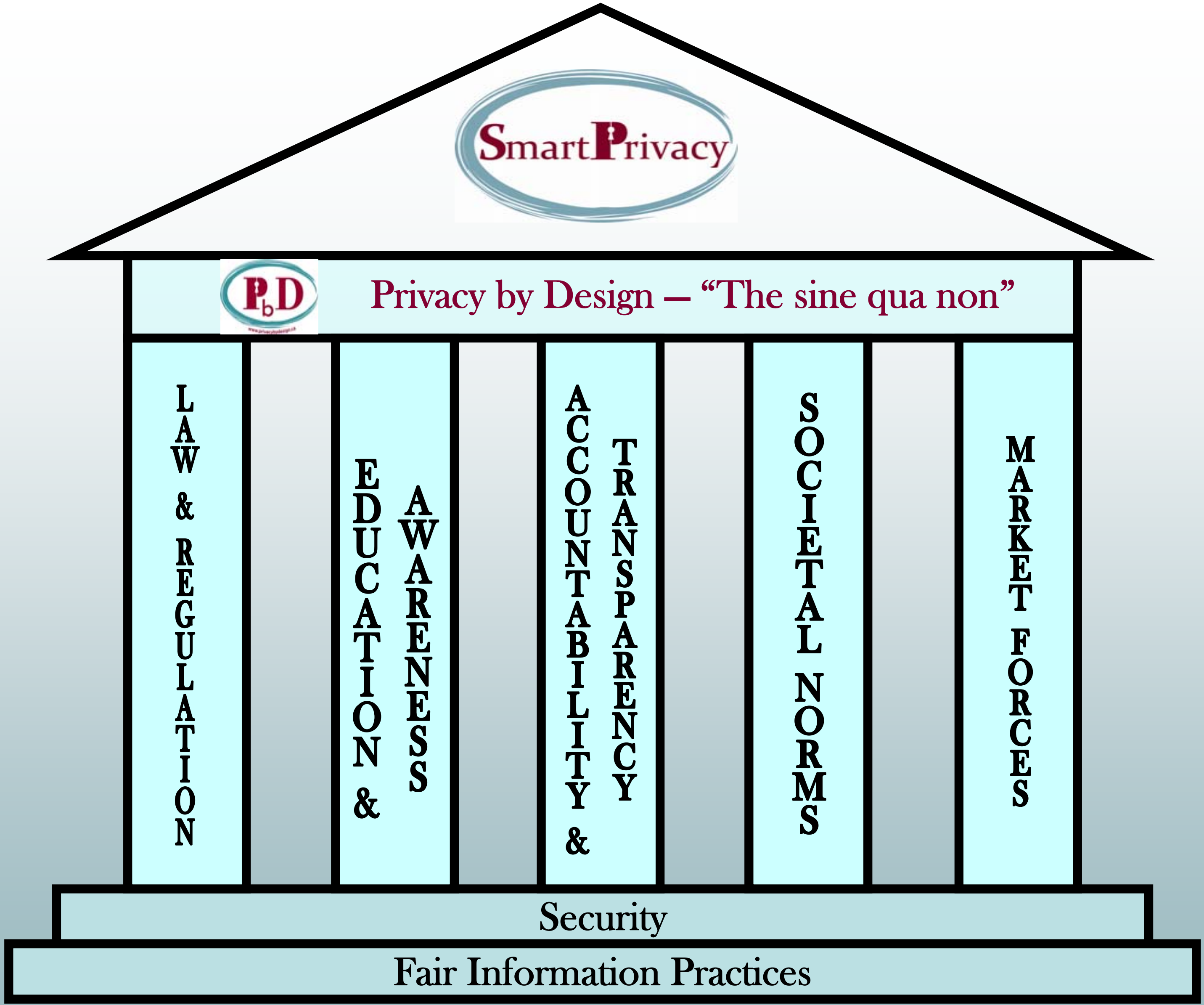
Positive-Sum Paradigm

- A **Zero-Sum Paradigm** describes a concept or situation in which one party’s gains are balanced by another party’s losses – win/lose; either/or; enhancing security often comes at the expense of privacy – the more you have of one, the less you can have of the other;
- A **Positive-Sum Paradigm**, in contrast, describes a situation in which *all* participants may gain together (win-win);
- To achieve a positive-sum model, privacy must be proactively built into the system so that privacy protections are engineered directly into the technology, right from the outset;
- The effect is a minimization of the unnecessary collection and use of personal data by the system, while at the same time, strengthening data security, and empowering individuals to exercise greater control;
- This can result in technologies that achieve strong security *and* privacy, delivering a “win-win” outcome.

Positive-Sum Model

Change the paradigm
from zero-sum to
a “positive-sum” model:
Create a win-win scenario,
not an either/or
involving unnecessary trade-offs
and false dichotomies

Get Smart About Privacy: *SmartPrivacy*



SmartPrivacy

PbD

Privacy by Design – "The sine qua non"

LAW & REGULATION

EDUCATION & AWARENESS

ACCOUNTABILITY & TRANSPARENCY

SOCIETAL NORMS

MARKET FORCES

Security

Fair Information Practices

"SmartPrivacy is the umbrella that offers the complete suite of protections to ensure data privacy. It consists of multiple measures ranging from regulatory protections to education and awareness, but one measure stands out as the sine qua non: *Privacy by Design*. *Dr. Ann Cavoukian, Information & Privacy Commissioner of Ontario, Canada, August 13, 2009.*

PbD
www.privacybydesign.ca

Privacy by Design: “Build It In”

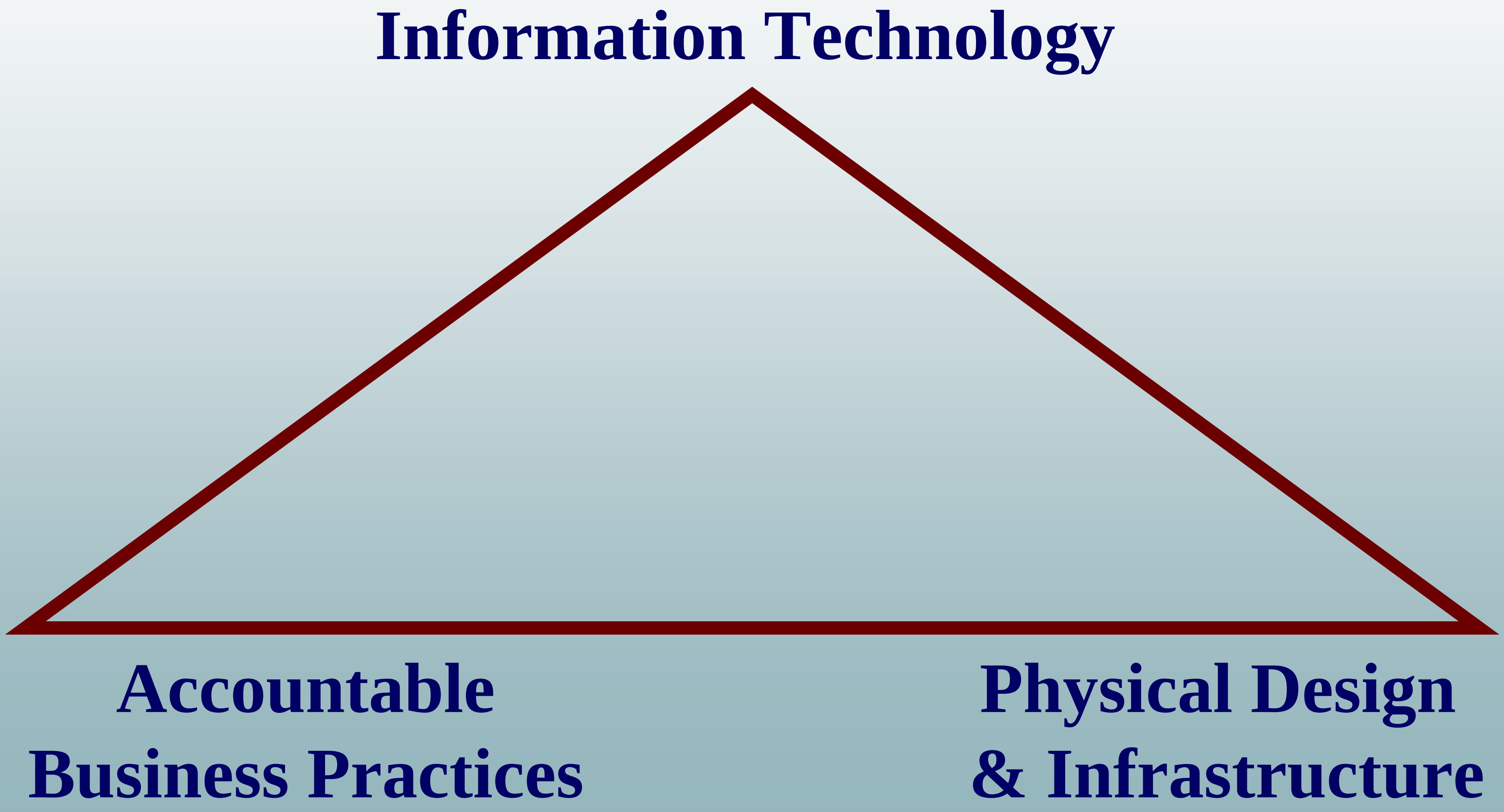
- I first developed the term “Privacy by Design” in the ‘90s, as a response to the growing threats to online privacy that were beginning to emerge;

- “Privacy by Design” seeks to build in privacy – up front, right into the design specifications; into the architecture; 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



Information Technology

Accountable
Business Practices

Physical Design
& Infrastructure

Privacy by Design:
Focus for 2009

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

Accountable Business Practices –
the 2nd Rung of PbD

***“You can outsource services …
but you can’t outsource Accountability.
You always remain accountable.”***

SmartPrivacy and the Smart Grid

Smart Grid:
What is It?

- The smart grid refers to an electricity system that monitors and optimizes its interconnected elements (e.g., generators, high-voltage networks, energy storage installations, and end-use consumers including household appliances and devices);
- A smart meter is a meter that can record and report electricity consumption information automatically;
- In our jurisdiction of Ontario, old hydro meters which used to be read in person are being replaced by a smart meter.

Ontario’s Smart Meter Initiative

- The Government of Ontario has committed to install a smart electricity meter in all homes and small businesses by the end of 2010 – *Energy Conservation Responsibility Act, 2006*;
- Smart meters will record electricity consumption on an hourly basis and report that information via a wireless technology;
- Individuals will be able to access their meter data from the previous day and be able to make choices about how to take advantage of future rates;
- A ‘smart metering entity’ (the Independent Electricity System Operator, or IESO) will receive and process the hourly consumer consumption data transmitted daily;
- The IESO is a listed institution under Ontario’s *FIPPA*.

Smart Grid:
Privacy Risks

- The information collected on a smart grid is a library of personal information, the mishandling of which could lead to the invasion of consumer privacy;
- An electricity usage profile could become a source of behavioural information;
- There will be major concerns if consumer-focused principles of transparency and control are not treated as essential design principles from start to end.

Smart Grid:
Where the IPC stands

- The smart grid is a good idea, but the focus is so much on controlling energy use that the privacy issue is understated. We must take care not to sacrifice consumer privacy amidst an atmosphere of enthusiasm for the project of electricity reform;
- Principles of *Privacy by Design* must be part of the overall design for smart grid data flows;
- Fortunately, for the people of Ontario, the government consulted with the IPC, and made its ‘smart metering entity’ subject to our jurisdiction.

RFID Transformed: Add an On/Off Device

RFID, Transformed: The Problem

- Privacy concerns arise when RFIDs are *associated with personally identifiable individuals;*
- Without appropriate security measures, embedding passive RFIDs into identity cards is problematic;
- The solution generally proposed – a protective sleeve, or Faraday Cage, is not sufficient.

The Problem (Cont'd)

- WHTI-compliant passcards and Enhanced Driver Licences (EDLs) contain passive RFID tags;
- These ID cards are being rolled out in border states and provinces, including Ontario;
- Our position: you should be able to turn the RFID off – the *default should be off* (the most privacy-protective option), unless the user chooses to turn it *on*, when needed.

RFID Transformed: The Solution

- We asked technology experts, ***how can you turn it off?***
- Impinj® Inc., (www.impinj.com), has developed a prototype Gen2 RFID Tag (TouchTag™) that functions only when activated by human touch – at a distance of up to 30 feet (9 metres);
- The tag remains *inoperative* (off) until the user touches a specific spot on the tag, which then enables the tag to be read;
- When the user releases his or her finger from the tag, it once again becomes inoperative – it turns off (which becomes the default);

* • **November 2, 2009** – Impinj® Inc. will be joining me in Madrid at the *Privacy by Design Workshop* where they will also have their RFID Tag technology on display – www.privacybydesign.ca/madrid09.htm

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” (false dichotomy);
- The future of privacy may very well depend on embedding privacy into design – let’s make it a reality.

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**

For more information on *Privacy by Design*, please visit
www.privacybydesign.ca