Deeply Embedded Privacy by Design

Ken Anderson
Assistant Commissioner (Privacy)
Ontario

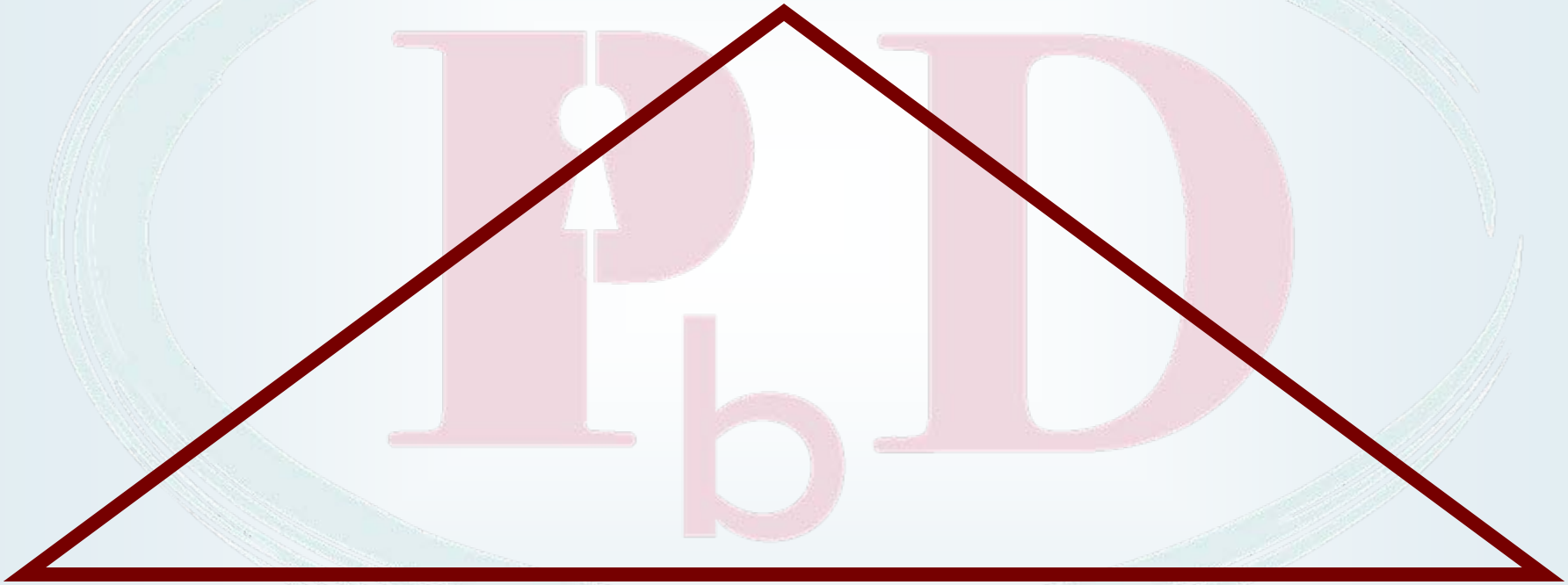
Identity, Privacy and Security Institute
University of Toronto
November 1, 2010

Presentation Outline

1. ***Privacy by Design: The Gold Standard***
2. **Privacy by Design for the Smart Grid**
3. **Wireless Sensors and Home Health Care**
4. **Questions and Answers**

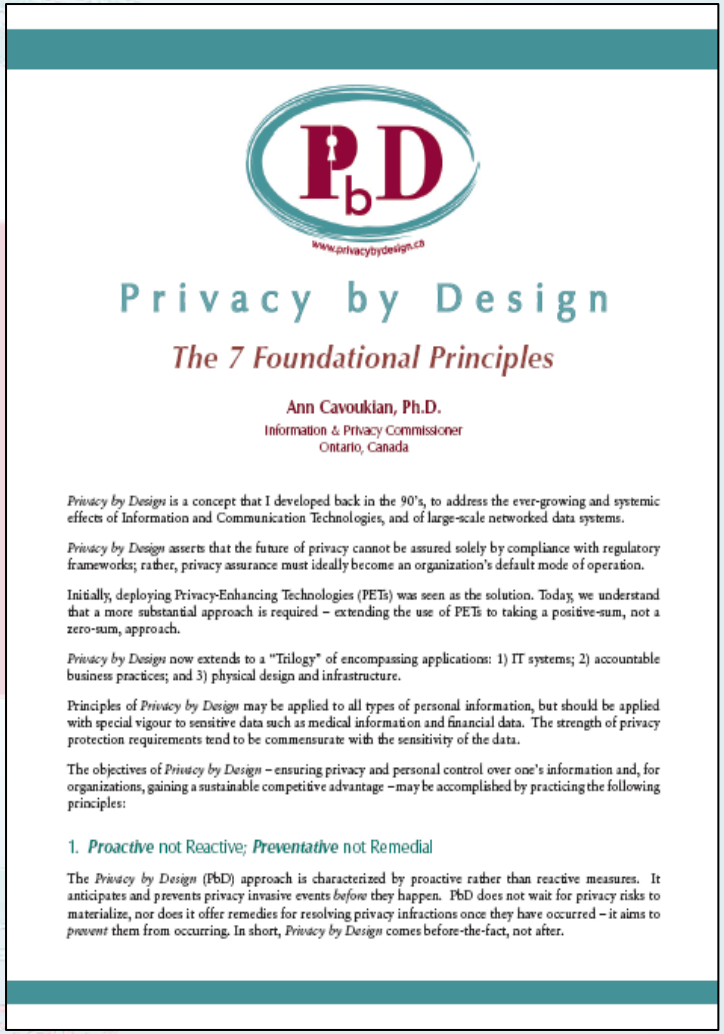

PbD
www.privacybydesign.ca

Privacy by Design:
The Trilogy of Applications



Privacy by Design:
The 7 Foundational Principles

1. *Proactive* not *Reactive;*
   Preventative not Remedial
2. Privacy as the *Default*
3. Privacy *Embedded* into Design
4. *Full* Functionality:
   Positive-Sum, *not* Zero-Sum
5. End-to-End Lifecycle
   Protection
6. Visibility and Transparency
7. Respect for User Privacy



PbD

www.privacybydesign.ca

Privacy by Design

The 7 Foundational Principles

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Privacy by Design is a concept that I developed back in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

Privacy by Design asserts that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we understand that a more substantial approach is required – extending the use of PETs to taking a positive-sum, not a zero-sum, approach.

Privacy by Design now extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and infrastructure.

Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy protection requirements tend to be commensurate with the sensitivity of the data.

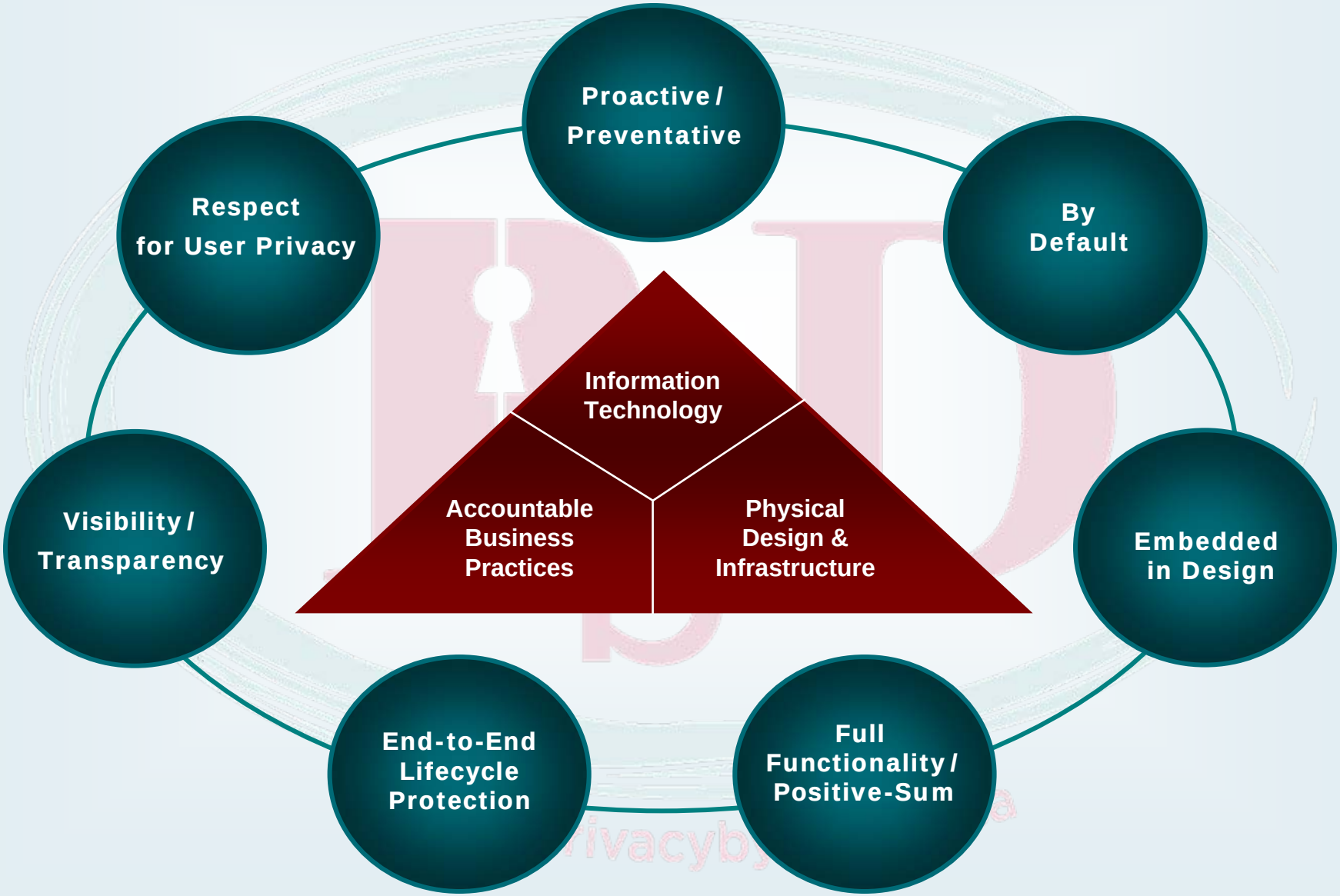
The objectives of *Privacy by Design* – ensuring privacy and personal control over one's information and, for organizations, gaining a sustainable competitive advantage – may be accomplished by practicing the following principles:

1. ***Proactive*** not Reactive; ***Preventative*** not Remedial

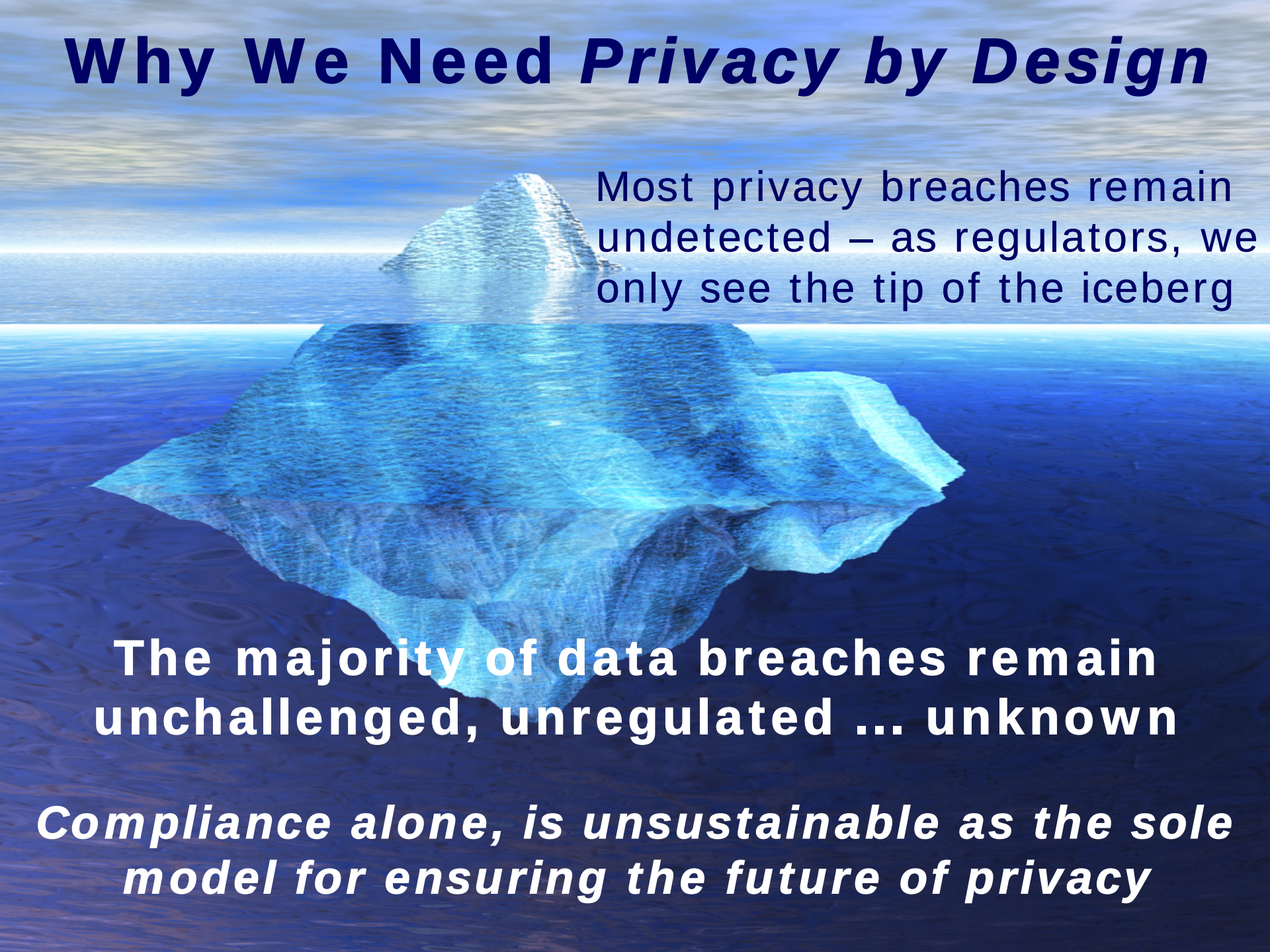
The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

PbD: The Next Wave in Privacy



Why We Need *Privacy by Design*



Most privacy breaches remain undetected – as regulators, we only see the tip of the iceberg

The majority of data breaches remain unchallenged, unregulated … unknown

Compliance alone, is unsustainable as the sole model for ensuring the future of privacy

Embedding Privacy at the Design Stage

- *Cost-effective*
- *Proactive*
- *User-centric*
- *It's all about control*
  - *personal control over data flows*

Achieving Consumer Trust and Freedom in the Information Age

"Privacy is good for business" is a mantra of the IPC that has, within 15 years, become a legal, market and functional requirement, not only for businesses but for ALL organizations — public, private and non-profit — that handle personal information;

The proposition is straightforward: build privacy into your data management systems from the outset and reap the many rewards of enhanced trust and consumer confidence;

The new realities and challenges of the Information Age require more robust fair information practices to be applied to a wide range of application scenarios, in multiple jurisdictions around the world. Privacy by Design, as reflected in the 7 Foundational Principles, respond directly to this need."

— Commissioner Ann Cavoukian, Ph.D.,
Privacy by Design: Achieving Consumer Trust and Freedom in the Information Age

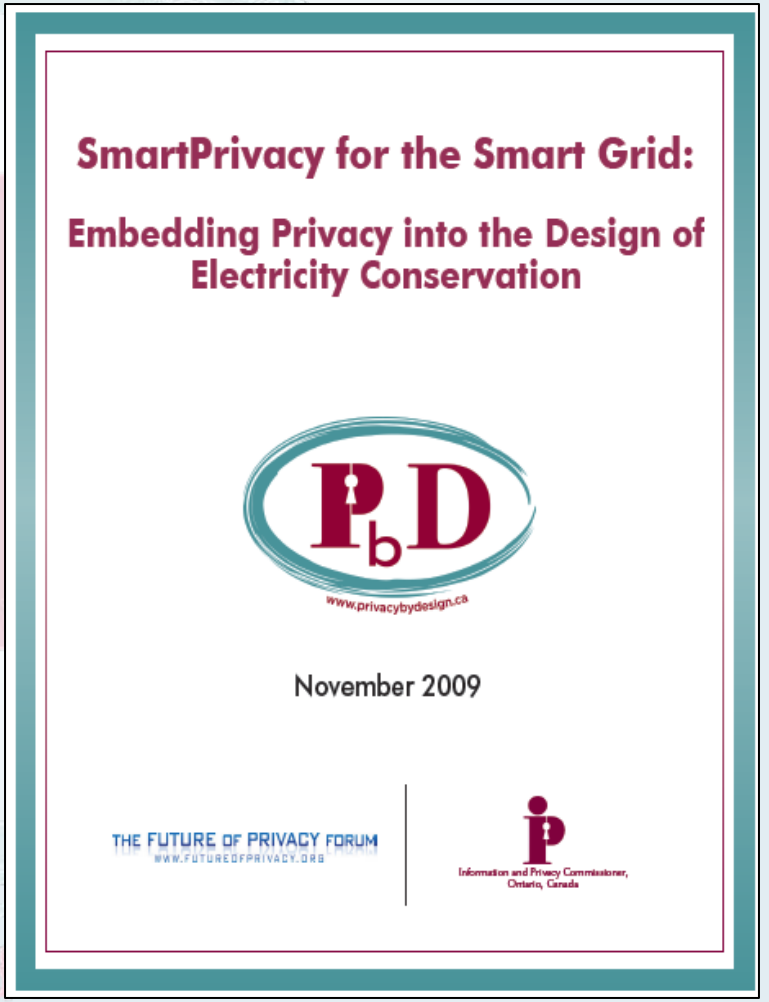
Upcoming article for Management Ethics (Autumn 2010)
www.ethicscentre.ca

SmartPrivacy for the Smart Grid:

Embedding Privacy into the Design of Electricity Conservation

"The smart grid is certainly a good idea, which I strongly support. But the focus has been so singularly on controlling energy use that I think the privacy issue is a sleeper – it is not top-of-mind."

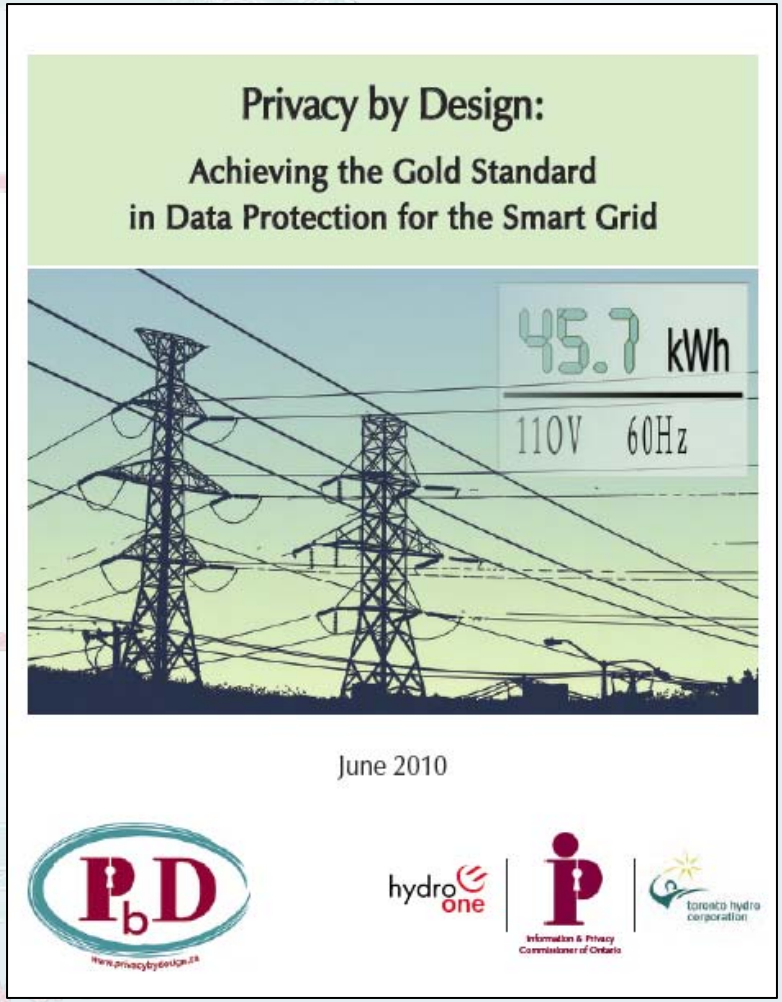
— Commissioner Cavoukian, Toronto Star, *Smart grid saves power, but can it thwart hackers?,* August 3, 2009



www.privacybydesign.ca

Privacy by Design:
Achieving the Gold Standard in Data Protection for the Smart Grid

- The Smart Grid in Ontario;
- Personal Information on the Smart Grid;
- *Privacy by Design*: The Gold Standard;
- ***Best Practices for the Smart Grid: Think Privacy by Design;***
- Smart Grid *Privacy by Design* Use Case Scenarios.



www.privacybydesign.ca

Jerusalem – October 25, 2010

Smart Grid Privacy 101:
Privacy by Design *in Action*
Power Morning

Jerusalem

www.privacybydesign.ca

PbD

Smart Grid Privacy 101:
Privacy by Design *in Action*
Power Morning

Crowne Plaza, Jerusalem > Monday, October 25, 2010 > 8:00 – 10:00 a.m.

The Smart Grid presents new opportunities for growth and change. As well, it presents new challenges related to the collection of customer energy consumption data. Sophisticated utilities recognize the transformative nature of the Smart Grid and are taking steps to address the privacy issues that will inevitably arise. Their forward-thinking approach embraces the "Positive-Sum" principle of Dr. Cavoukian's *Privacy by Design* because it optimizes the interests of both electrical reform and privacy.

If you are a privacy regulator or professional, this two-hour seminar will provide you with tested, practical guidance enabling you to work with energy providers and utilities, ensuring the protection of personal information contained within the Smart Grid. Energy providers will also be interested to hear the first hand account of Hydro One's — Ontario's largest electricity company — implementation of a *Privacy by Design* Smart Grid.

Follow us at www.twitter.com/embedprivacy

Information & Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Canada

www.privacybydesign.ca

PbD

SmartGrid Research Data Warehouse

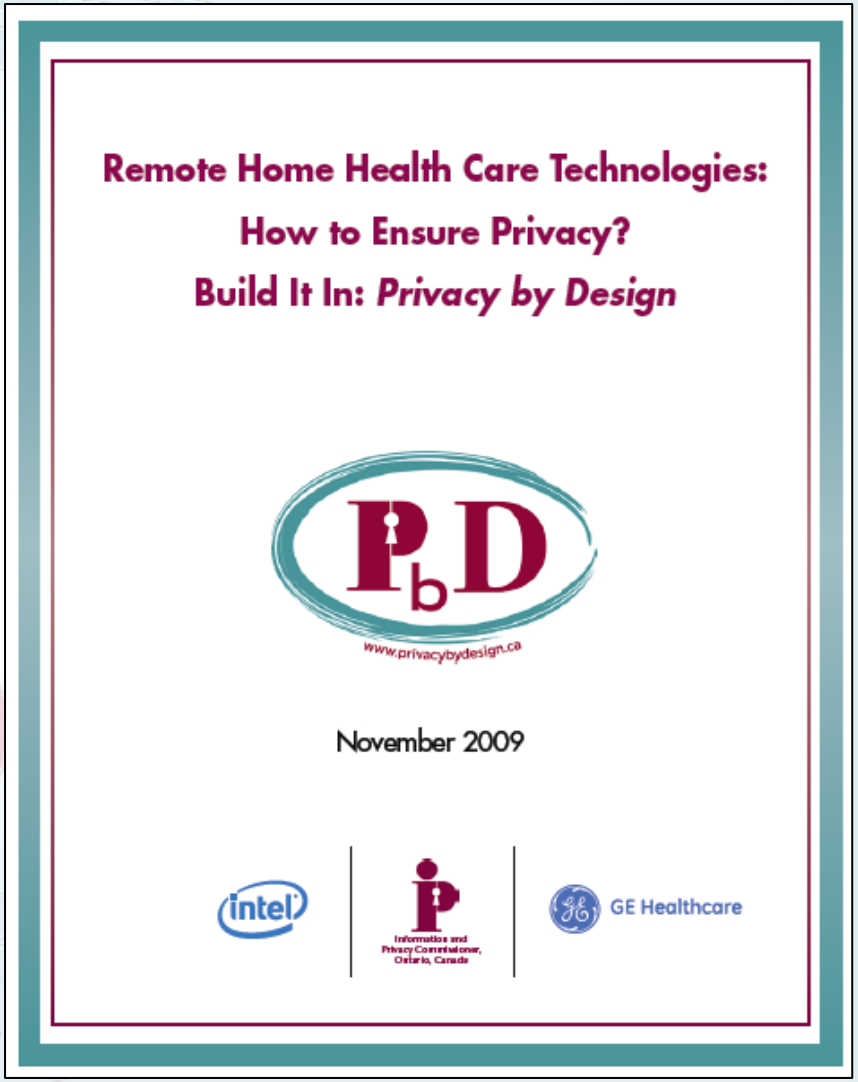
- In September 2010, the IPC was approached by the University of Toronto to assist in the creation of a research data warehouse that will utilize smart meter data to enhance the goals of the Smart Grid;
- We would play an advisory role based on our understanding of Ontario's advanced metering infrastructure and background in privacy;
- This project will support innovation in Ontario and Canada, creating new commercial opportunities to ensure that Canadian companies remain competitive in this expanding global arena.

Coming Soon:
New IPC Smart Grid Publications

- **Smart Grid *Privacy by Design***:
  A European Perspective, with Dr. Alexander Dix, Commissioner for Data Protection and Freedom of Information, Berlin, Germany;
- **Operationalizing *Privacy by Design***:
  An Ontario Smart Grid Case Study with Hydro One, IBM, GE and Telvent – relating to the Ontario Smart Grid pilot project (due January, 2011).

Remote Home Health Care Technologies

- Data Transmission and Analysis
- Privacy and Remote Home Health Care
- Fair Information Practices
- Practical Application
- GE's QuietCare and Intel's Health Guide



www.ipc.on.ca

Sensors and In-Home Collection of Health Data

- Building in Privacy
- Positive-Sum Paradigm
- IATSL's COACH and HELPER systems
- Applying Privacy by Design
- Focus on the User
- Focus on the Sensor System
- Focus on the Data

www.ipc.on.ca

Innovative Wireless Home Care

- Privacy and Personal Health Information
- We Care Home Health Services: Two Wireless Solutions Using BlackBerry® Smartphone
- Privacy Best Practices for Integrating Wireless Handheld Devices in the Delivery of Home Care

Discussion

Q's & A's

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