

# THE IAPP PRIVACY ACADEMY 2010

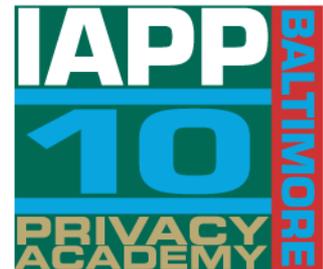
# *Practical Privacy by Design: A Hands On Workshop*

**Ken Anderson**

**Assistant Commissioner (Privacy)**

**Ontario**

*September 29, 2010*



# Presentation Outline

THE IAPP PRIVACY ACADEMY 2010

- 1. The Privacy Landscape*
- 2. Change the Paradigm*
- 3. Privacy by Design*
- 4. Privacy by Design in Action:  
The Smart Grid*
- 5. Conclusions*



# The Privacy Landscape



# Information Privacy Defined

THE IAPP PRIVACY ACADEMY 2010

**Freedom of choice – personal control**

**“Informational self-determination”**

**Fair Information Practices**

**Global Privacy Standard (2006)**

[www.ipc.on.ca/images/Resources/up-gps.pdf](http://www.ipc.on.ca/images/Resources/up-gps.pdf)



# *What Privacy is Not*

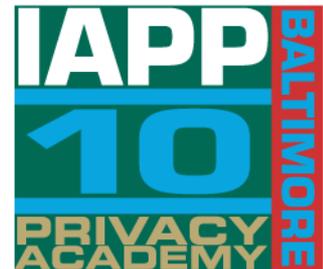
THE IAPP PRIVACY ACADEMY 2010

# Privacy $\neq$ Security

*Security is, however, vital to privacy*



# *Change the Paradigm*

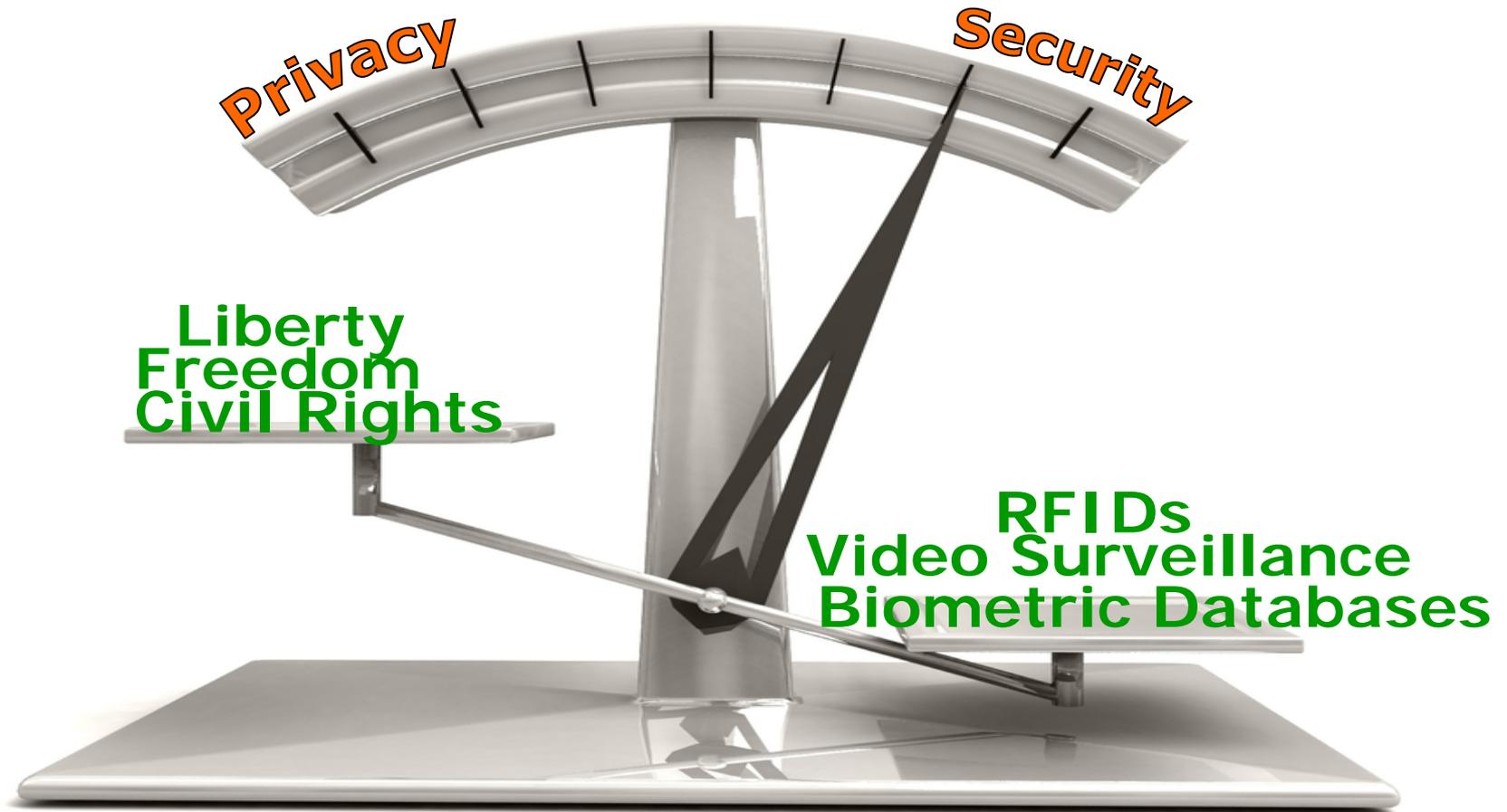


*If Privacy is to Survive,  
Things Have to Change*



*Change the Paradigm to  
Positive-Sum,  
**NOT**  
Zero-Sum*

# *The Zero-Sum Approach*



# Positive-Sum Model

THE IAPP PRIVACY ACADEMY 2010

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



# *Privacy by Design*



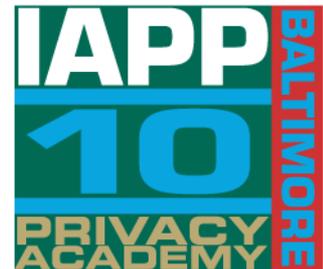
# Privacy by Design: *The Trilogy of Applications*

THE IAPP PRIVACY ACADEMY 2010

## Information Technology

Accountable  
Business Practices

Physical Design  
& Infrastructure



# Privacy by Design: The 7 Foundational Principles

THE IAPP PRIVACY ACADEMY 2010

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

[www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf](http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf)



## 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.

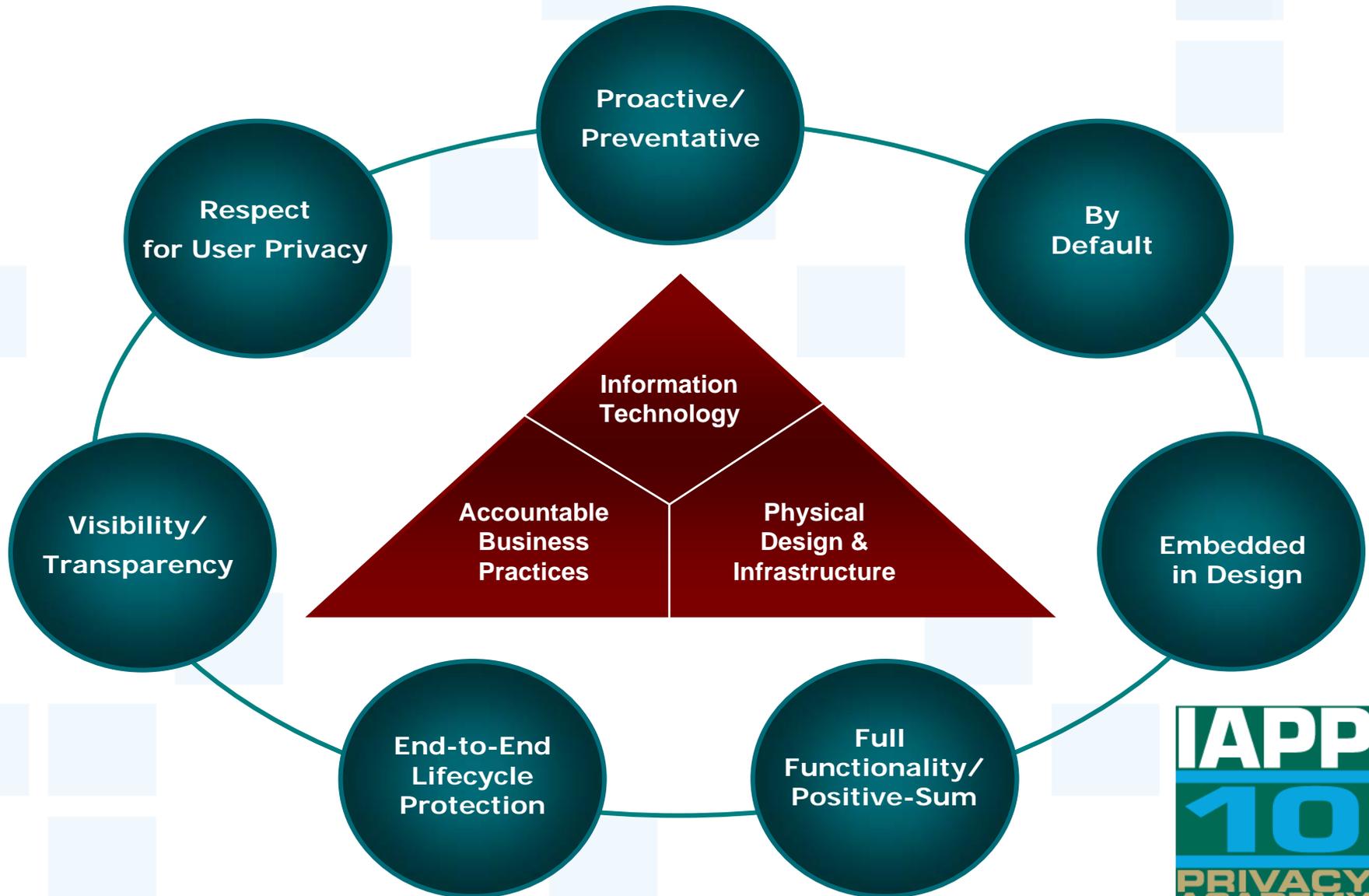
The objectives of *Privacy by Design* – ensuring privacy and personal control over one's information and, for organizations, gaining a sustainable competitive advantage – may be accomplished by practicing the following principles:

#### 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.

# *PbD: The Next Wave in Privacy*

THE IAPP PRIVACY ACADEMY 2010



# 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***



[www.privacybydesign.ca](http://www.privacybydesign.ca)

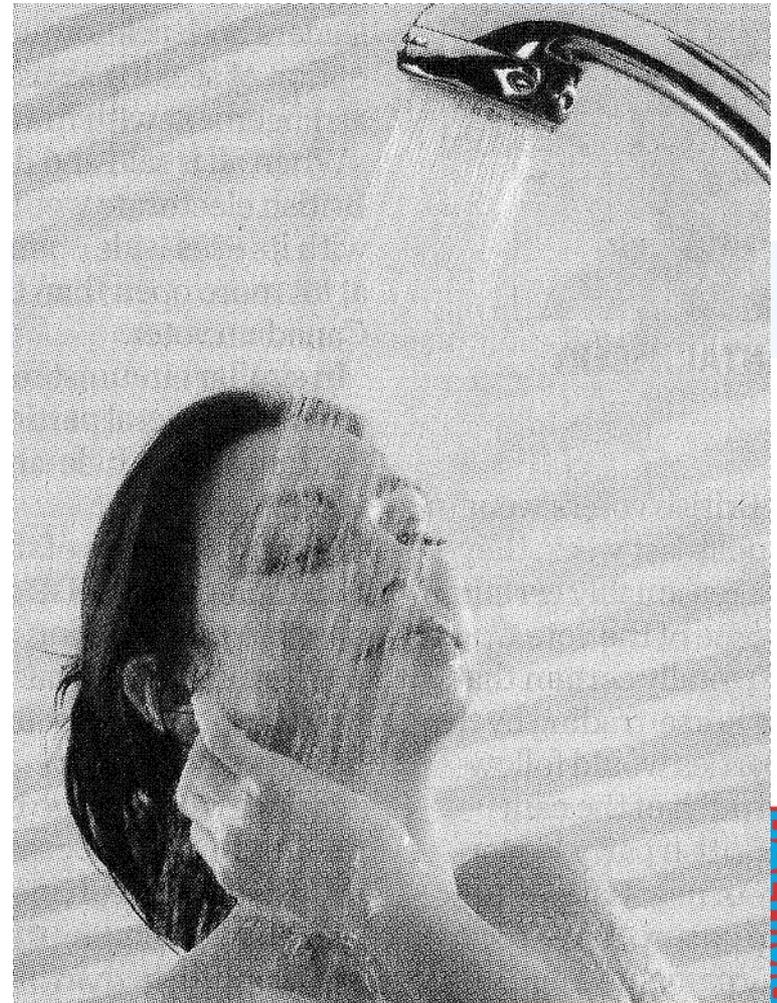


# *Privacy by Design* in Action:

## The Smart Grid

# Can the Smart Grid Know Too Much?

THE IAPP PRIVACY ACADEMY 2010



**PRIVACY  
ACADEMY**

**BALTIMORE**

# Personally Identifiable Information and the Smart Grid

THE IAPP PRIVACY ACADEMY 2010

- Modernization of the current electrical grid will involve end-user components and activities that will lead to increasing the collection, use and disclosure of personal information by utility providers, as well as third-parties
- What constitutes “personal information” on the Smart Grid is the subject of much discussion
- In the context of the Smart Grid, the linkage of any personally identifiable information with energy use would render the linked data as personal information and privacy considerations immediately apply

# Smart Grid: Privacy Risks

THE IAPP PRIVACY ACADEMY 2010

- An electricity usage profile can translate into a source of detailed behavioural information
- Digital data is vulnerable to unauthorized access, copying, matching, merging and widespread dissemination for secondary purposes without the consent of the consumer

# Smart Grid: Privacy Risks

THE IAPP PRIVACY ACADEMY 2010

- Actual cases show that even data that has been anonymized is at risk of re-identification
- Potential insider threats within utilities and third parties

# Personal Privacy Must Remain Paramount

THE IAPP PRIVACY ACADEMY 2010

*"So far, Ontario is leading the game, but the modernization of the grid is in its infancy and if vigilance isn't maintained, personal habits could become everyone's business."*

— Commissioner Cavoukian

*"We've taken the advice of the privacy commissioner upfront before the smart grid is even put in place."*

— Brad Duguid,  
Ontario Minister of Energy and  
Infrastructure

**Toronto Star, May 12, 2010**

04-200 WEDNESDAY, MAY 12, 2010 • TORONTO STAR • A23 CANADA

## Can smart grid know too much?

Hydro meter info a boon for thieves, marketers, and must be protected, privacy czar says

**THEY KNOW WHEN YOU ARE SLEEPING ...**



**THEY KNOW WHEN YOU'RE AWAKE ...**



**THEY KNOW WHEN YOU'RE IN THE SHOWER**



Imagine the enormous interest in this information — not only by marketers and companies but unauthorized third parties like the bad guys, thieves who'll know when you are not at home," Cavoukian said in an interview.

Now is the time to continue to install privacy safeguards around the grid as it grows, she said.

So far, Ontario is "leading the game," she said. But the modernization of the grid is in its infancy and if vigilance isn't maintained, personal habits could become everyone's business.

Energy Minister Brad Duguid said he is taking Cavoukian's advice "very seriously" and is putting measures in place by controlling who has access to the information.

"We've taken the advice of the privacy commissioner upfront before the smart grid is even put in place," he said.

Yet before the switch was flicked on the program, all bases should have been examined and covered, said Progressive Conservative energy critic MPP John Yakubuk.

"We've talked about them having a serious rethink about smart meters from the get-go and every day we find more reasons why they should be doing that," Yakubuk said.

The infrastructure supporting the smart grid system will be soon be capable of letting consumers know their hourly and real-time energy use, Cavoukian said. "They can develop patterns of behaviour when you are away from the home," she said. "This thing has to be protected like Fort Knox."

In the not-so-distant future, "smart" appliances will be able to send in even more gory details on how we live our lives to companies that provide electrical power. The sharing of that data should concern consumers, Cavoukian said.

"Think about every single appliance in your house reporting, in real time, your energy use. What will develop over time is a library of personal information relating to a profile of your personal energy use. When you watch TV, what time of day when you eat, when you sleep and when," she said.

Ontario must stay proactive on this, she said. "Right now is the ideal time to ensure no one gets this information other than the people who get it now — Toronto Hydro and Hydro-Quebec."

The privacy commissioner is working with both on how electrical companies should set standards. The companies will not give out any personal data without the consent of the consumer, she said.

"This is a treasure trove of information. We want to make sure privacy is the default."

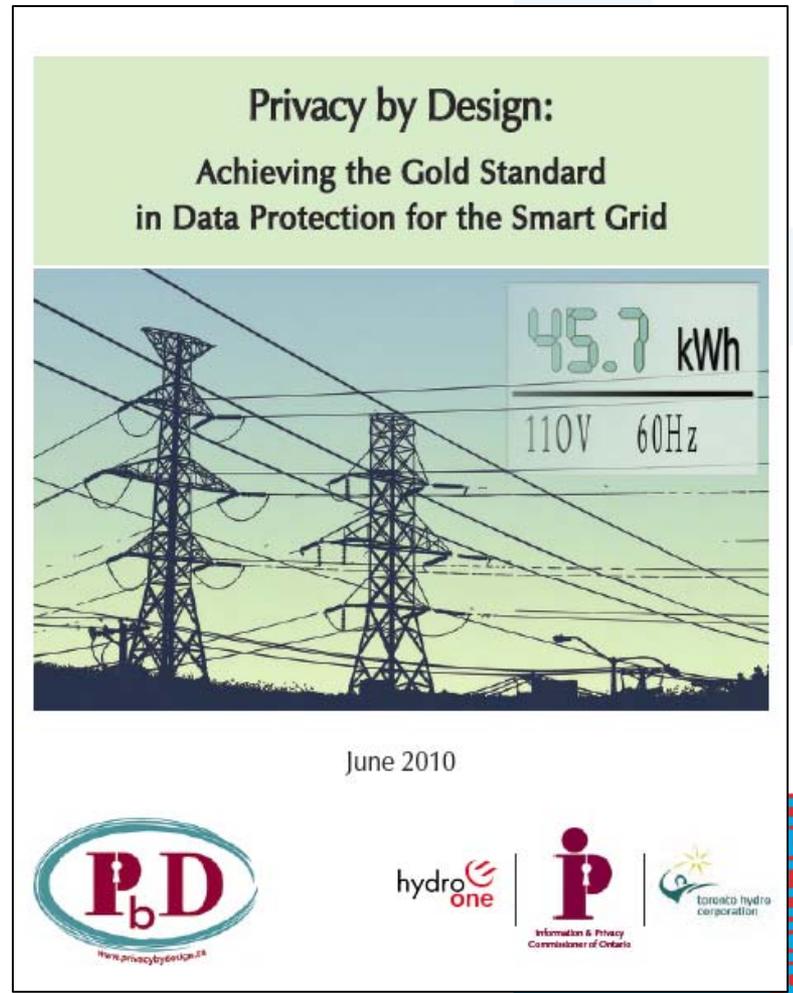
<http://tinyurl.com/24dzn9j>

PRIVACY

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

THE IAPP PRIVACY ACADEMY 2010

- 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



# Jerusalem – October 25, 2010

## Smart Grid Privacy 101: Privacy by Design *in Action*

Power Morning

# Jerusalem



[www.privacybydesign.ca](http://www.privacybydesign.ca)



## 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](http://www.twitter.com/embedprivacy)



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

[www.privacybydesign.ca](http://www.privacybydesign.ca)



# Smart Grid *Privacy by Design*: Ontario ... and Beyond

THE IAPP PRIVACY ACADEMY 2010

- Many jurisdictions, around the world, are starting to enter into Smart Grid initiatives
- Utilities, embarking upon Smart Grid initiatives involving the collection of personally identifiable information, will benefit from the ***Best practices for Smart Grid Privacy by Design***
- Other jurisdictions will also benefit from Ontario's experience with building ***Privacy by Design*** into the foundational elements of all Smart Grid developments



# Conclusions

THE IAPP PRIVACY ACADEMY 2010

- Lead with *Privacy by Design*
- Change the paradigm from “zero-sum” to “positive-sum”
- Deliver *both* privacy AND security in a doubly enabling “win-win” paradigm
- Embed privacy as a core functionality: the future of privacy will depend on it!



# How to Contact Us

THE IAPP PRIVACY ACADEMY 2010

## **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](http://www.ipc.on.ca)

E-mail: [info@ipc.on.ca](mailto:info@ipc.on.ca)

