Privacy by Design – The Gold Standard: Bridging Privacy, Security and Trust

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario

Eighth Annual Conference on Privacy, Security and Trust

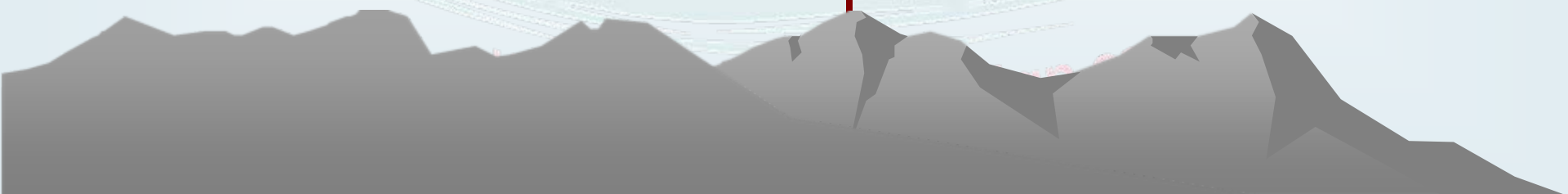
Ottawa, Canada

August 17, 2010

Presentation Outline

1. *The Privacy Landscape*
2. *Why We Need to Change the Paradigm*
3. *Positive-sum, NOT Zero-Sum*
4. *Privacy by Design*
5. *Advancing Privacy and Innovation*
6. *Conclusions*
7. *Appendix*

The Privacy Landscape



Privacy = Freedom

Information Privacy Defined

Freedom of choice – personal control

"Informational self-determination"

Fair Information Practices

Global Privacy Standard (2006)

www.ipc.on.ca/images/Resources/up-gps.pdf

What Privacy is Not

Privacy ≠ Security

Security is, however, vital to privacy

Setting the Stage:

Why We Need to Change the Paradigm

If Privacy is to Survive, Things Have to Change

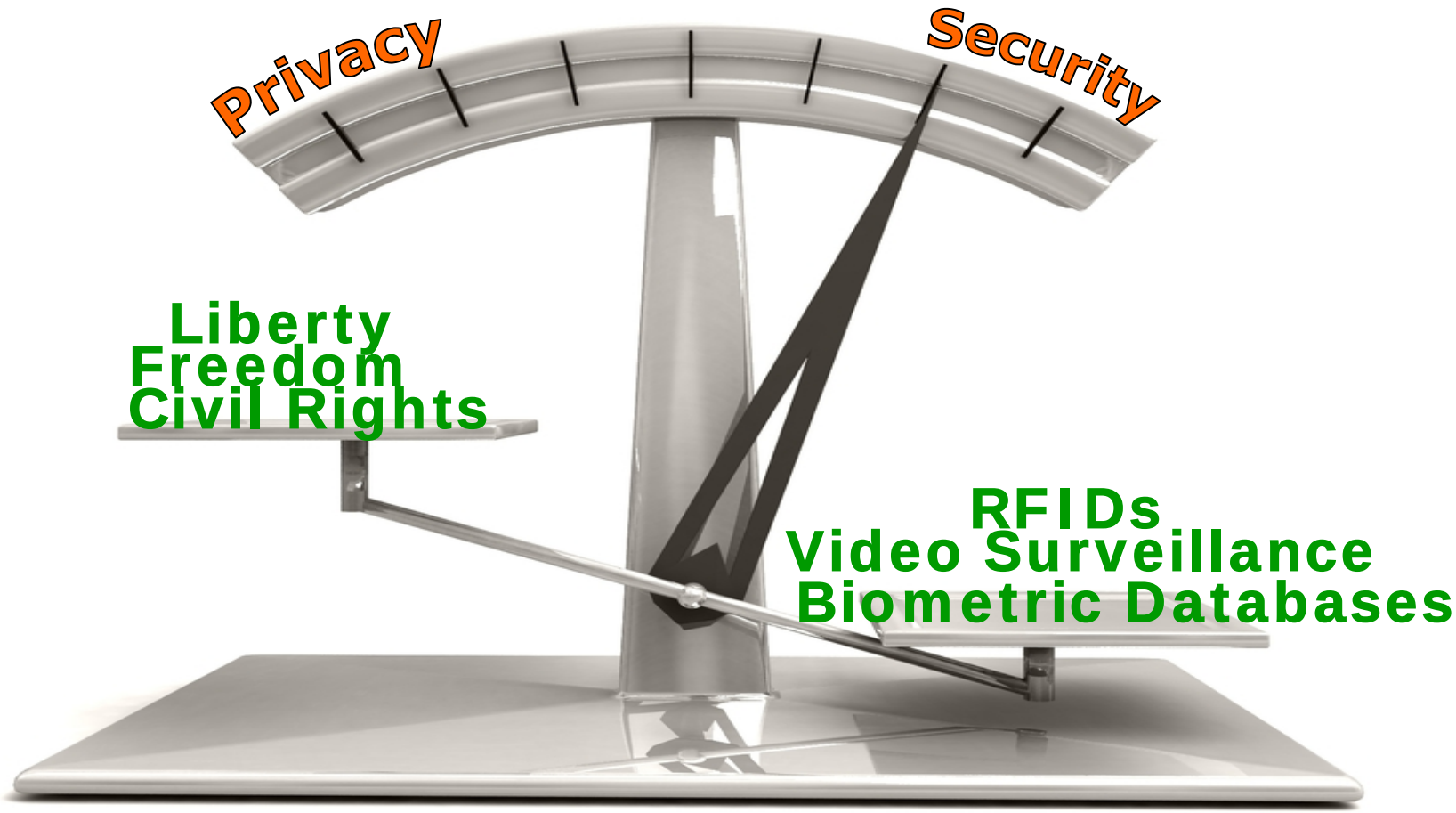
The Future of Privacy

Change the Paradigm to Positive-Sum,

NOT

Zero-Sum

The Zero-Sum Approach

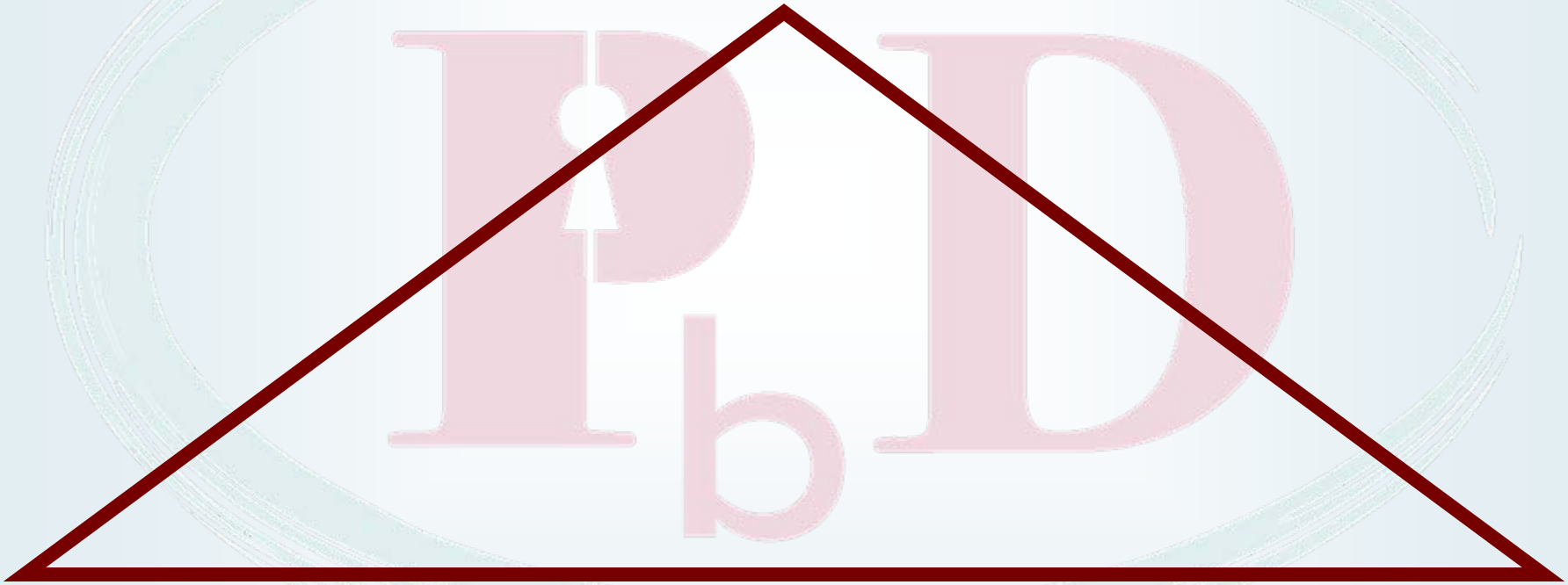



PbD
www.privacybydesign.ca

Positive-Sum Model

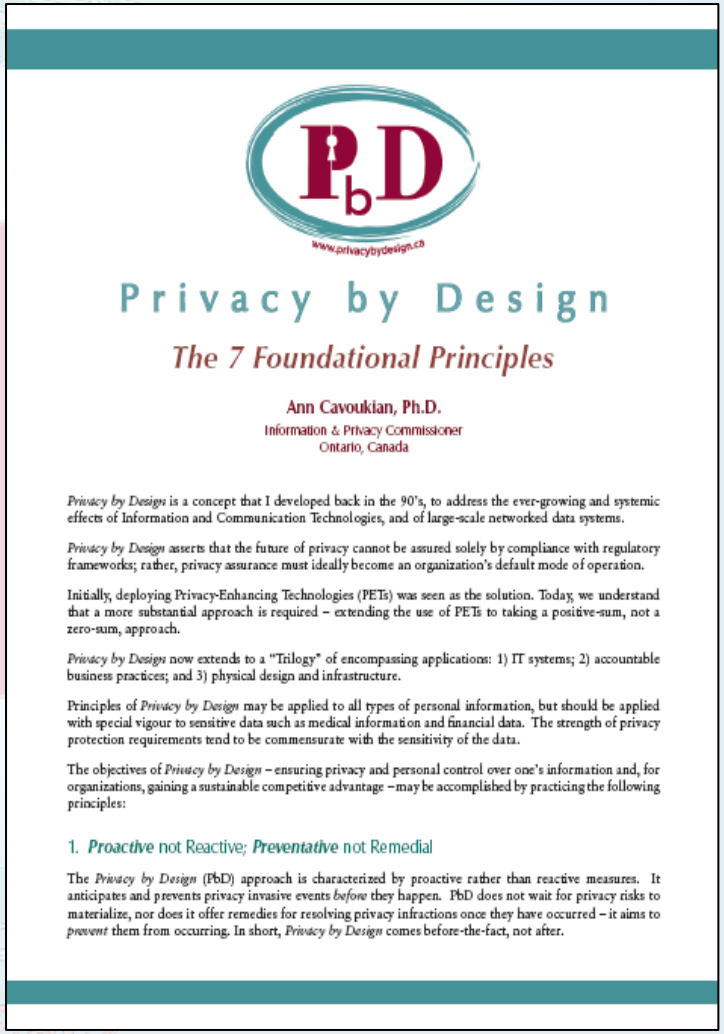
Change the paradigm from a zero-sum to a "positive-sum" model: Create a win-win scenario, not an either/or involving unnecessary trade-offs and false dichotomies

Privacy by Design:
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.

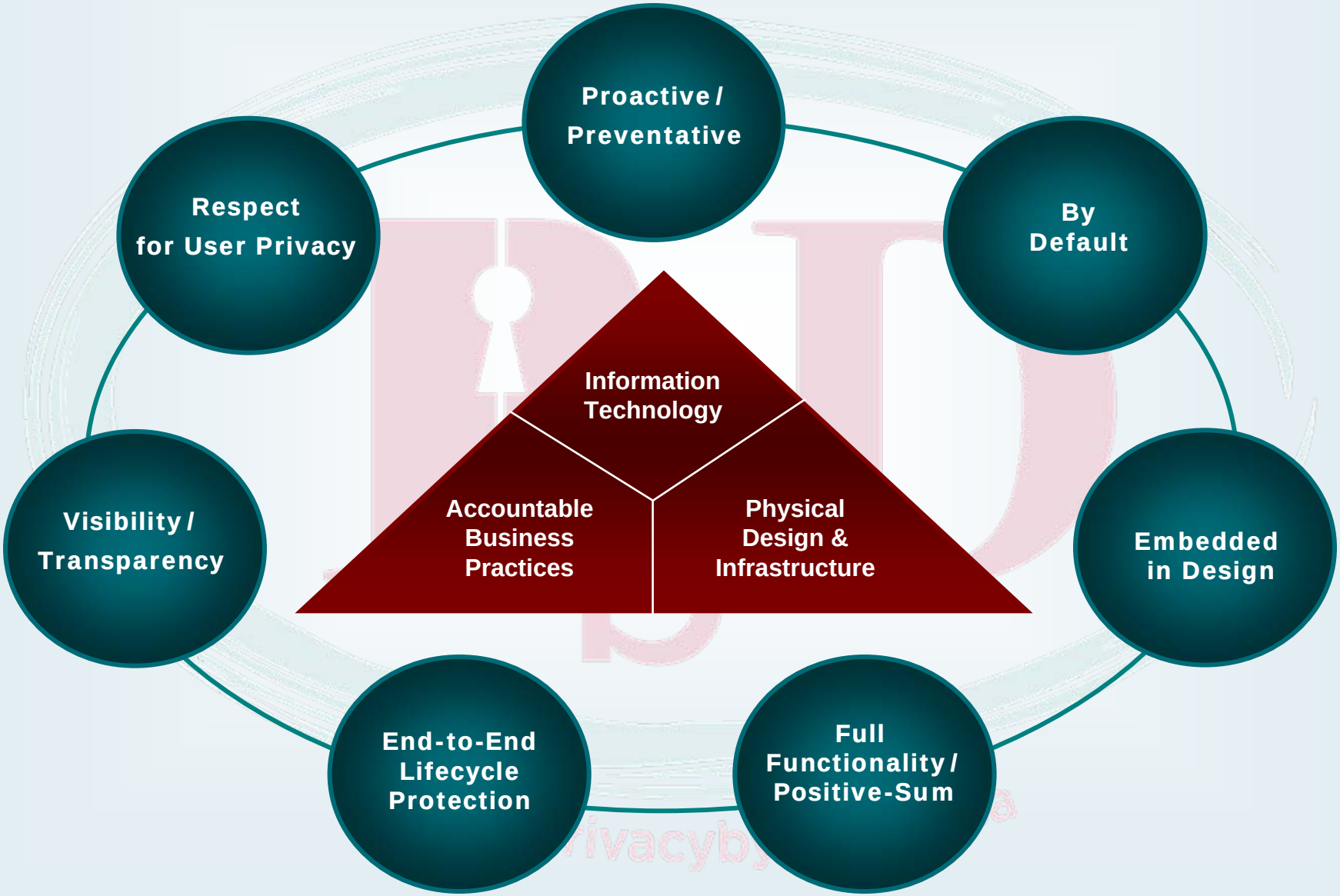
The objectives of *Privacy by Design* – ensuring privacy and personal control over one's information and, for organizations, gaining a sustainable competitive advantage – may be accomplished by practicing the following principles:

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

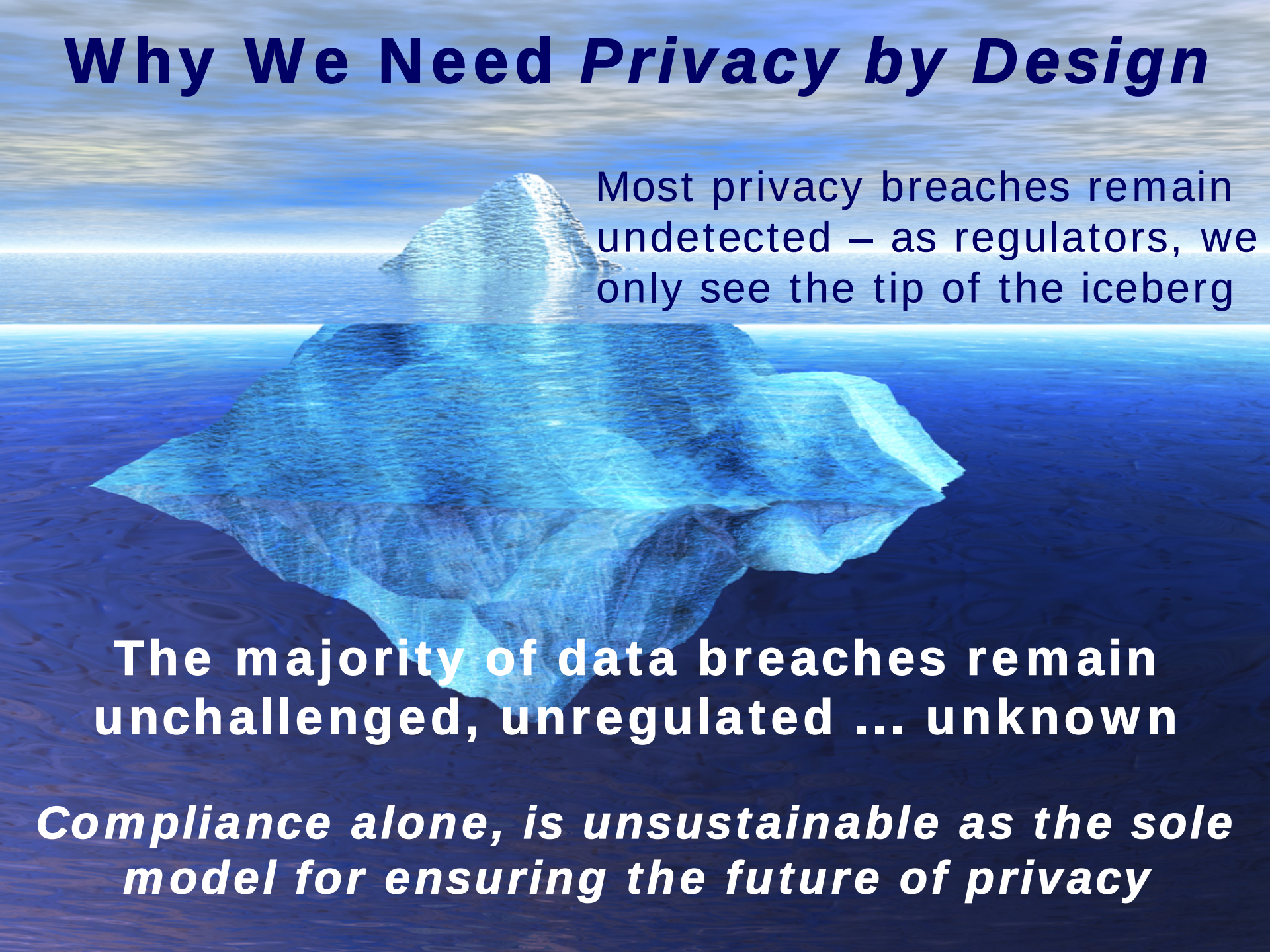
The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have 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*

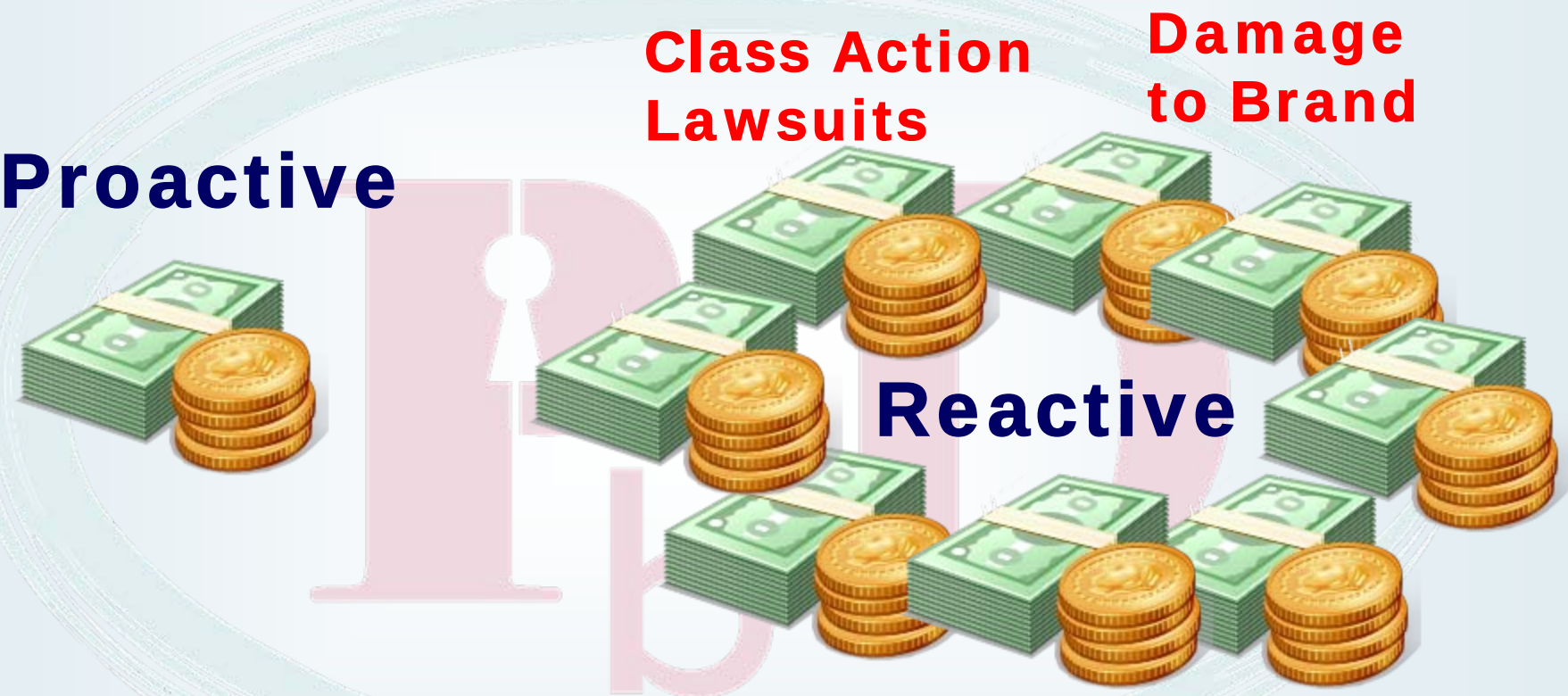


Most privacy breaches remain undetected – as regulators, we only see the tip of the iceberg

The majority of data breaches remain unchallenged, unregulated … unknown

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

Cost of Taking a Reactive vs. Proactive Approach to Privacy Breaches



... You do the Math

Bottom Line:
It's All About Trust

"Trust is more important than ever online … Price does not rule the Web … Trust does."

— Frederick F. Reichheld,
Loyalty Rules: How Today's Leaders Build Lasting Relationships

Embedding Privacy at the Design Stage

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

Privacy by Design
in Action

The Need for Smart Grid Privacy

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

TANYA TALAGA
QUEEN'S PARK BUREAU

The time you jump into the shower in the morning, the time you finally flick off that TV at night – even the time you set your home security alarm.

Ontario's privacy czar wants to keep the information secret.

Personal privacy must remain paramount as the "smart grid" electricity system is built around the province, said Ann Cavoukian, Ontario's information and privacy commissioner.

As the grid collects information on power usage and smart meters are installed in Ontario homes to track consumption data, that personal information could represent a treasure trove for hackers, thieves or marketers, said Cavoukian, in her annual report released Tuesday.

"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 Yakabuski.

"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," Yakabuski 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 gritty 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 wake," 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 One."

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."

THEY KNOW WHEN YOU ARE SLEEPING ...

SHUTTERSTOCK IMAGE

THEY KNOW WHEN YOU'RE AWAKE ...

RICHARD LAUTENS/TORONTO STAR FILE PHOTO

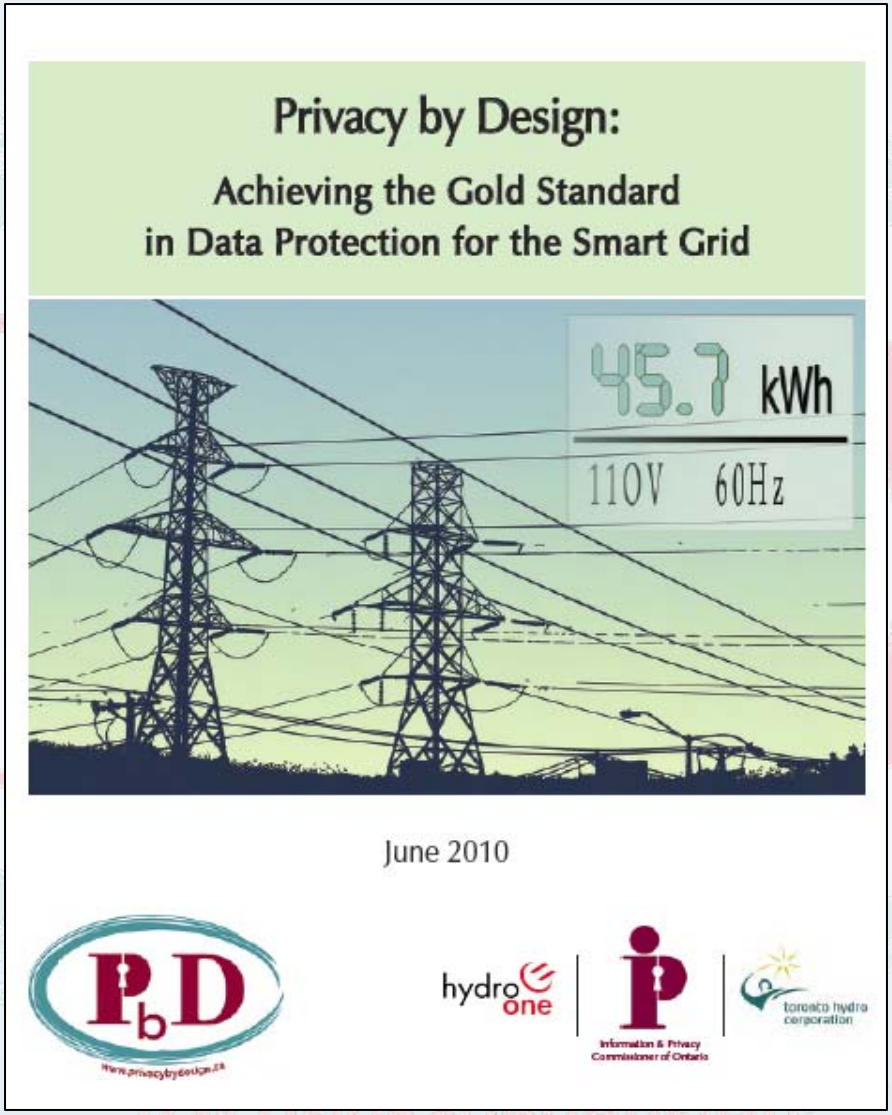
THEY KNOW WHEN YOU'RE IN THE SHOWER

SHUTTERSTOCK IMAGE

What time you sleep, cook, shower, turn on the TV, or set the alarm system can be tracked by the province's emerging smart grid hydro system, possibly tipping off thieves to a household's habits. "This thing has to be protected like Fort Knox," says Ontario's privacy commissioner Ann Cavoukian.

Toronto Star, May 12, 2010 - http://tinyurl.com/24dzn9j

Smart Grid Privacy



www.ipc.on.ca/images/Resources/achieve-goldstnd.pdf0

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

Advancing Privacy and Innovation

Identity, Privacy and Security Institute
University of Toronto

IPSI is dedicated to developing new approaches to security that maintain the privacy, freedom and safety of the individual and the broader community

Engineering – Mathematics – Computer Sciences – Information Studies

www.ipsi.utoronto.ca

The Next Evolution in Data Protection:

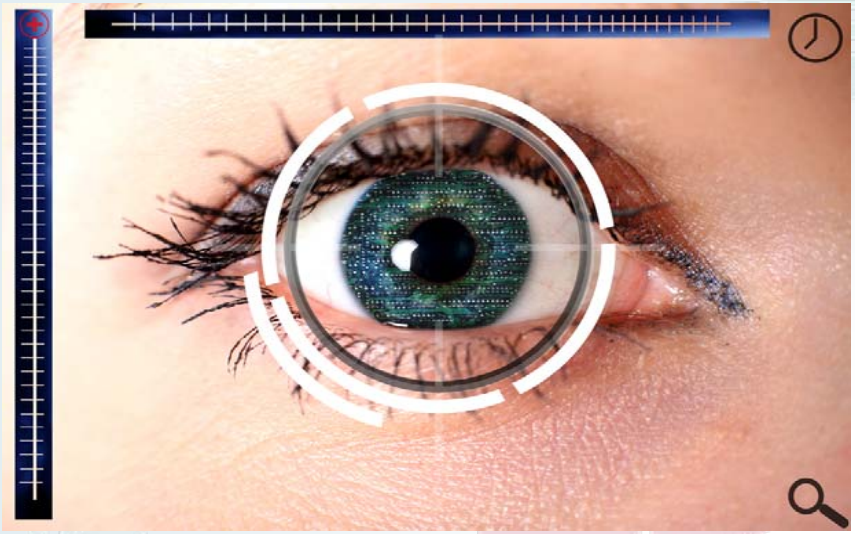
"SmartData"

Developed at IPSI, *SmartData* represents the future of privacy and the control of personal information online

Intelligent or "smart agents" introduced into IT systems virtually – thereby creating "*SmartData,*"
– a new approach to Artificial Intelligence that will revolutionize the field.

www.ipc.on.ca/images/Resources/bio-encrypt-chp.pdf

Biometric Encryption



www.ipc.on.ca/images/Resources/untraceable-be.pdf

Fostering Privacy and Innovation at MaRS

Conclusions

- 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!

Appendix

- The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices (http://www.privacybydesign.ca/papers.htm)
- *Privacy by Design*: Achieving the Gold Standard in Data Protection for the Smart Grid (http://www.ipc.on.ca/images/Resources/achieve-goldstnd.pdf)
- Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security *AND* Privacy (*http://www.ipc.on.ca/index.asp?navid=46&fid1=608*)
- Wireless Communications Technologies: Video Surveillance Systems (*http://www.ipc.on.ca/index.asp?navid=46&fid1=626*)
- Fingerprint Biometrics: Address Privacy Before Deployment (*http://www.ipc.on.ca/index.asp?navid=46&fid1=816*)
- Fingerprint Biometric Systems: Ask the Right Questions Before You Deploy (*http://www.ipc.on.ca/index.asp?navid=46&fid1=769*)
- Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum not Zero-Sum (*http://www.ipc.on.ca/index.asp?navid=46&fid1=758*)
- Practical Tips for Implementing RFID Privacy Guidelines (*http://www.ipc.on.ca/index.asp?navid=46&fid1=430*)
- Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report - Privacy Investigation (*http://www.ipc.on.ca/index.asp?navid=53&fid1=7874*)
- Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines) (*http://www.ipc.on.ca/index.asp?navid=46&fid1=432*)
- RFID and Privacy: Guidance for Health-Care Providers (*http://www.ipc.on.ca/index.asp?navid=46&fid1=724*)
- What's New Again? Security Measures Must Be Real – Not Illusory (*http://www.ipc.on.ca/index.asp?navid=46&fid1=813*)
- The Relevance of Untraceable Biometrics and Biometric Encryption: A Discussion of Biometrics for Authentication Purposes (*http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=879*)
- Whole Body Imaging in Airport Scanners: Building in Privacy by Design (*http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=846*)
- Privacy by Design ... Take the Challenge *(http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=856)*

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