Get Smart About Privacy: Privacy by Design – The Gold Standard

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario

Identity, Privacy and Security Institute

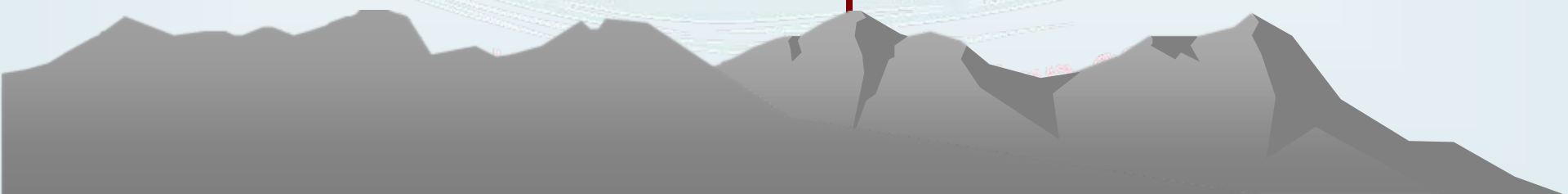
University of Toronto

November 19, 2010

Presentation Outline

1. *The Privacy Landscape*
2. *Why We Need to Change the Paradigm*
3. *The Future of Privacy: My Prediction*
4. *Privacy by Design: The Gold Standard*
5. *Smart Grid Privacy:*
   Privacy by Design in Action
6. *Use Case Scenarios*
7. *Conclusions*

The Privacy Landscape



Privacy = Freedom

Information Privacy Defined

Freedom of choice
– personal control over one's data flows

"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

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

The Future of Privacy: My Prediction

My Prediction

"The world has less than a decade to make the protection of personal information and online privacy a priority before the concepts are lost forever … online privacy problems will only worsen if governments don't take a hard stance."

— Commissioner Cavoukian,
Ottawa Citizen, August 18, 2010

World is losing grip on privacy: watchdog

Next decade will be crucial in protecting personal data

BY VITO PILIECI

The world has less than a decade to make the protection of personal information and online privacy a priority before the concepts are lost forever, warns Ontario's information and privacy commissioner.

Ann Cavoukian says legislation meant to safeguard privacy already can't keep pace with the flow of information and advances in technology.

"We have a large job to do," she told about 100 people Tuesday at a conference at the University of Ottawa.

"This is sort of a David vs. Goliath thing."

Cavoukian's call comes as Facebook, Google and other companies have been forced to examine how they handle personal data.

Facebook in particular has been under the microscope of privacy advocates around the world who have criticized the social networking company for sharing too much of the personal information of members with marketing firms.

Google was caught collecting private Wi-Fi data in 30 countries in June. The Internet company, which claims the data collection was unintentional, also has been forced to repeatedly defend its StreetView mapping service, which many complain is too invasive.

BRUNO SCHLUMBERGER, OTTAWA CITIZEN

'It's your information, you should be able to decide what happens to it.'

ANN CAVOUKIAN
Ontario's information and privacy commissioner

Cavoukian said online privacy problems will worsen if governments don't take a hard stance.

Several tools are being used by hackers to steal personal data by tricking consumers into viewing websites infected with worms and viruses, and there are still no laws in place forcing private companies to disclose when personal information, such as credit card details, has been breached.

See PRIVACY on PAGE A2

Actual Prediction:
Only One Decade Remains

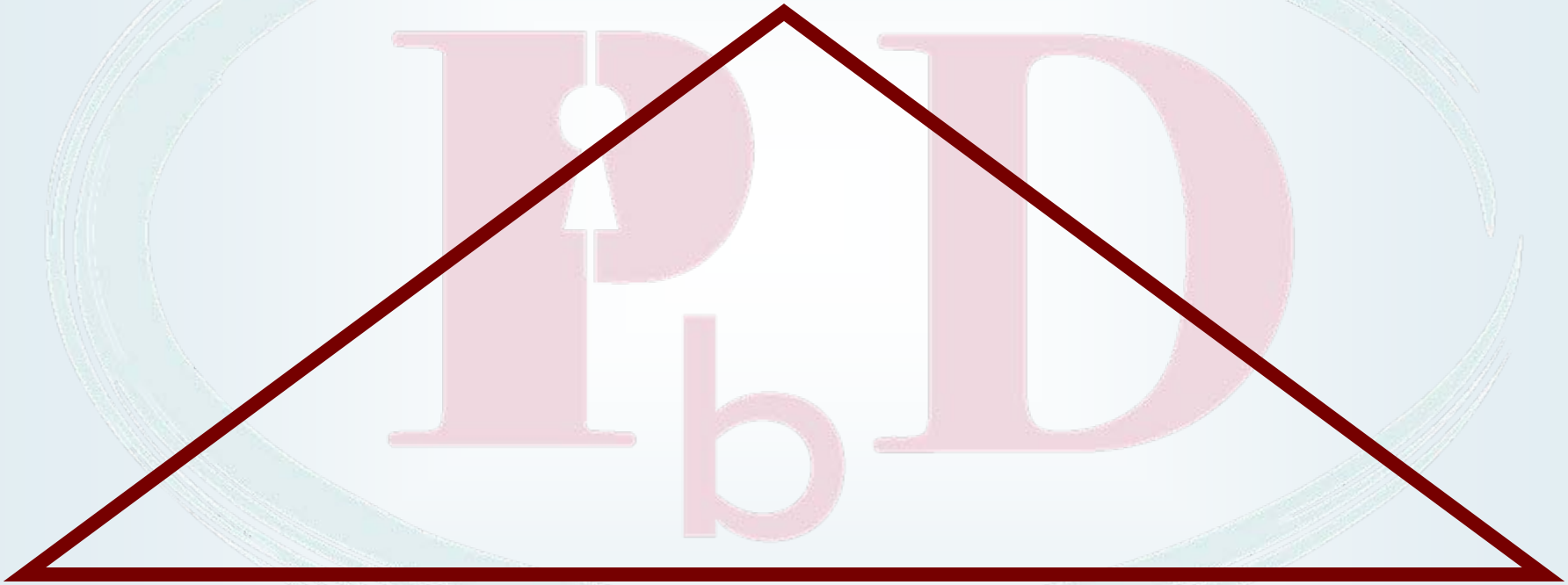
"Unless we act now, I predict that privacy, as we know it, will be gone – lost, beyond our grasp, by the year 2020."

— Commissioner Cavoukian,
International Conference of Data Protection and Privacy Commissioners,
Jerusalem, October 28, 2010.


PbD
www.privacybydesign.ca

Privacy by Design:
The Trilogy of Applications

Information Technology

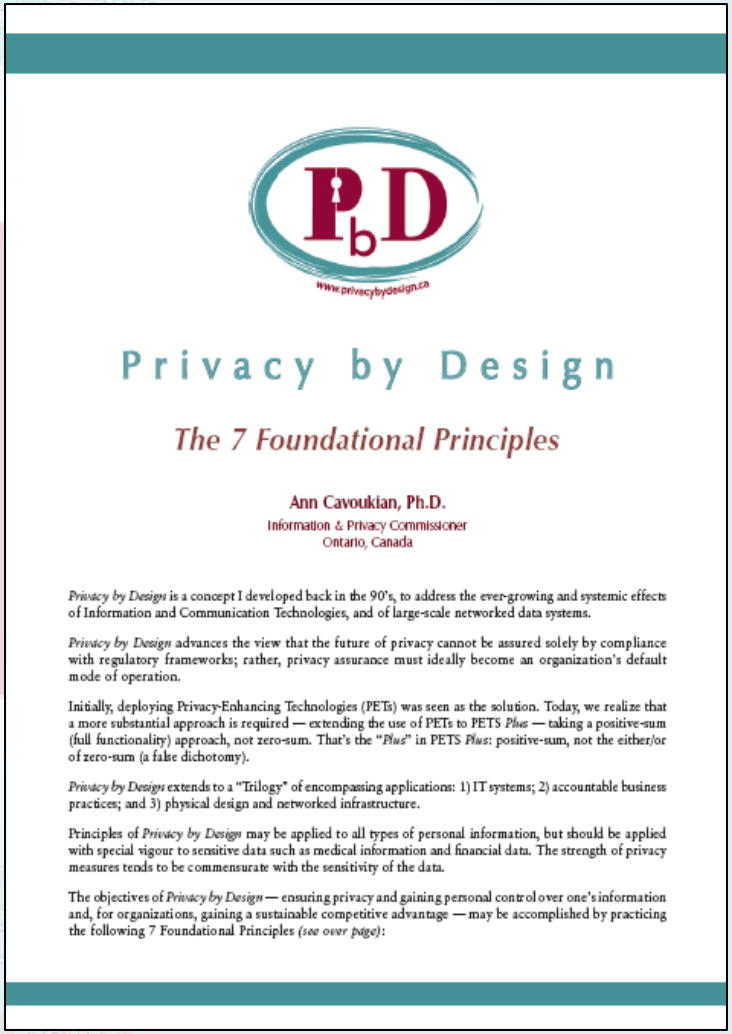


Accountable Business Practices

Physical Design & Infrastructure

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 **Security**:
   Lifecycle Protection;
6. Visibility **and** Transparency;
7. Respect for User Privacy:
   Keep it User-Centric.



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 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 advances the view 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 realize that a more substantial approach is required — extending the use of PETs to PETS *Plus* — taking a positive-sum (full functionality) approach, not zero-sum. That's the "*Plus*" in PETS *Plus*: positive-sum, not the either/or of zero-sum (a false dichotomy).

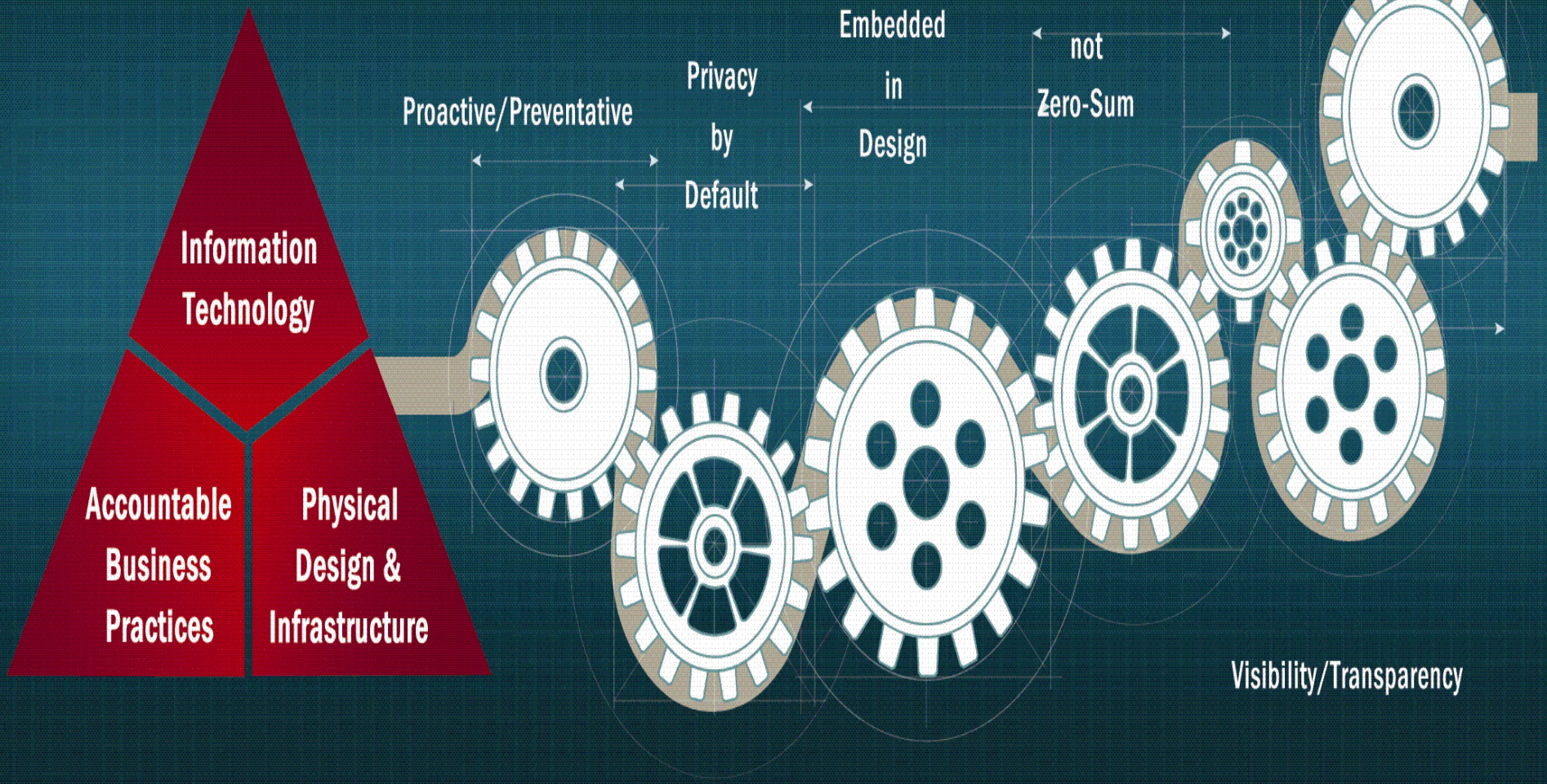
Privacy by Design extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure.

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 measures tends to be commensurate with the sensitivity of the data.

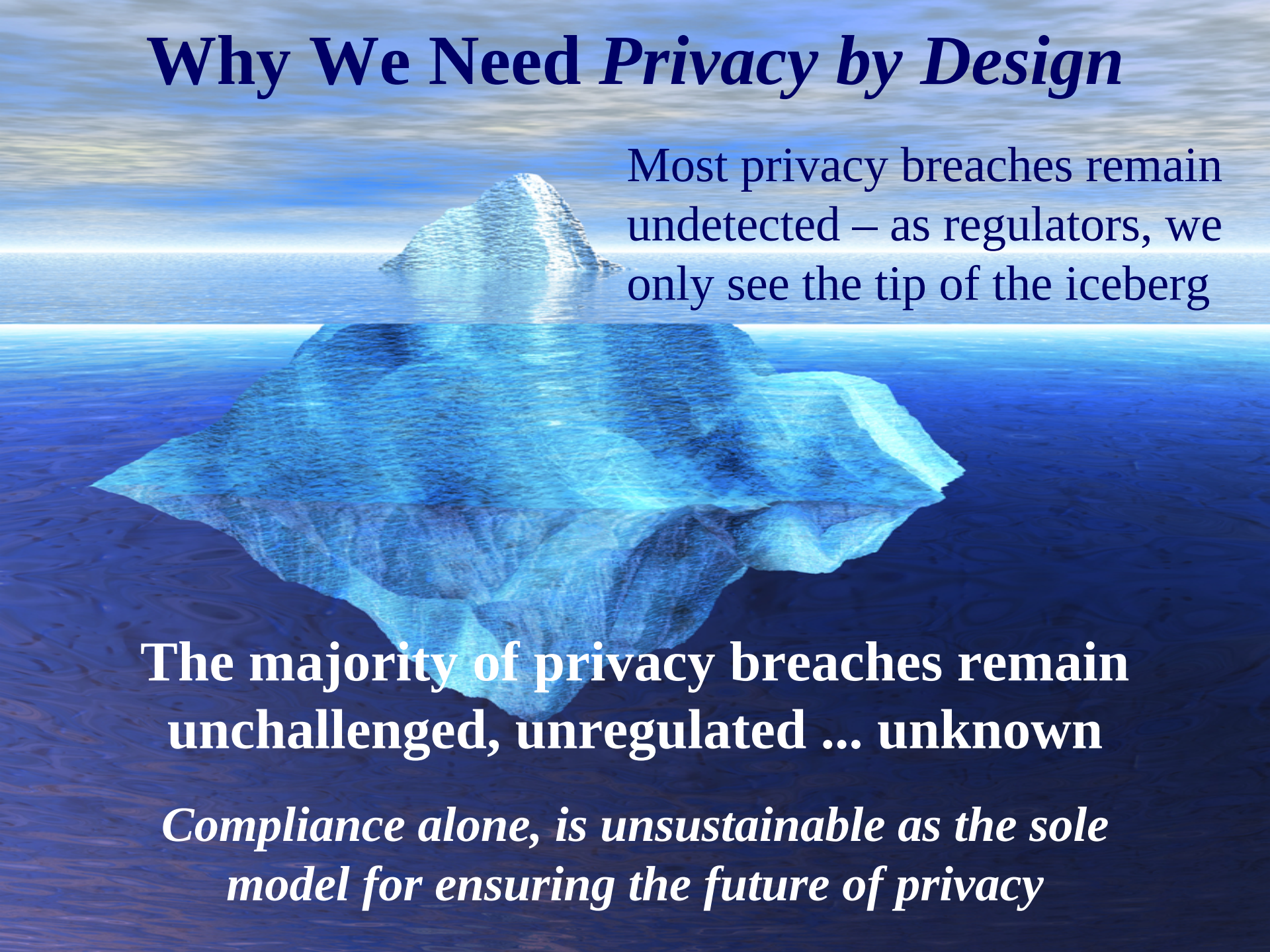
The objectives of *Privacy by Design* — ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following 7 Foundational Principles *(see over page)*:

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

Privacy by Design



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 ... unknown

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

Adoption of "Privacy by Design" Resolution

Landmark Resolution Passed to Preserve the Future of Privacy

By Anna Ohlden – October 29th 2010 - http://www.science20.com/newswire/landmark_resolution_passed_preserve_future_privacy

TORONTO, October 29, 2010 /PRNewswire – A landmark resolution by Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, was approved by international Data Protection and Privacy Commissioners in Jerusalem today at their annual conference. The resolution recognizes Commissioner Cavoukian's concept of Privacy by Design - which ensures that privacy is embedded into new technologies and business practices, right from the outset - as an essential component of fundamental privacy protection.

Full Article:

http://www.science20.com/newswire/landmark_resolution_passed_preserve_future_privacy

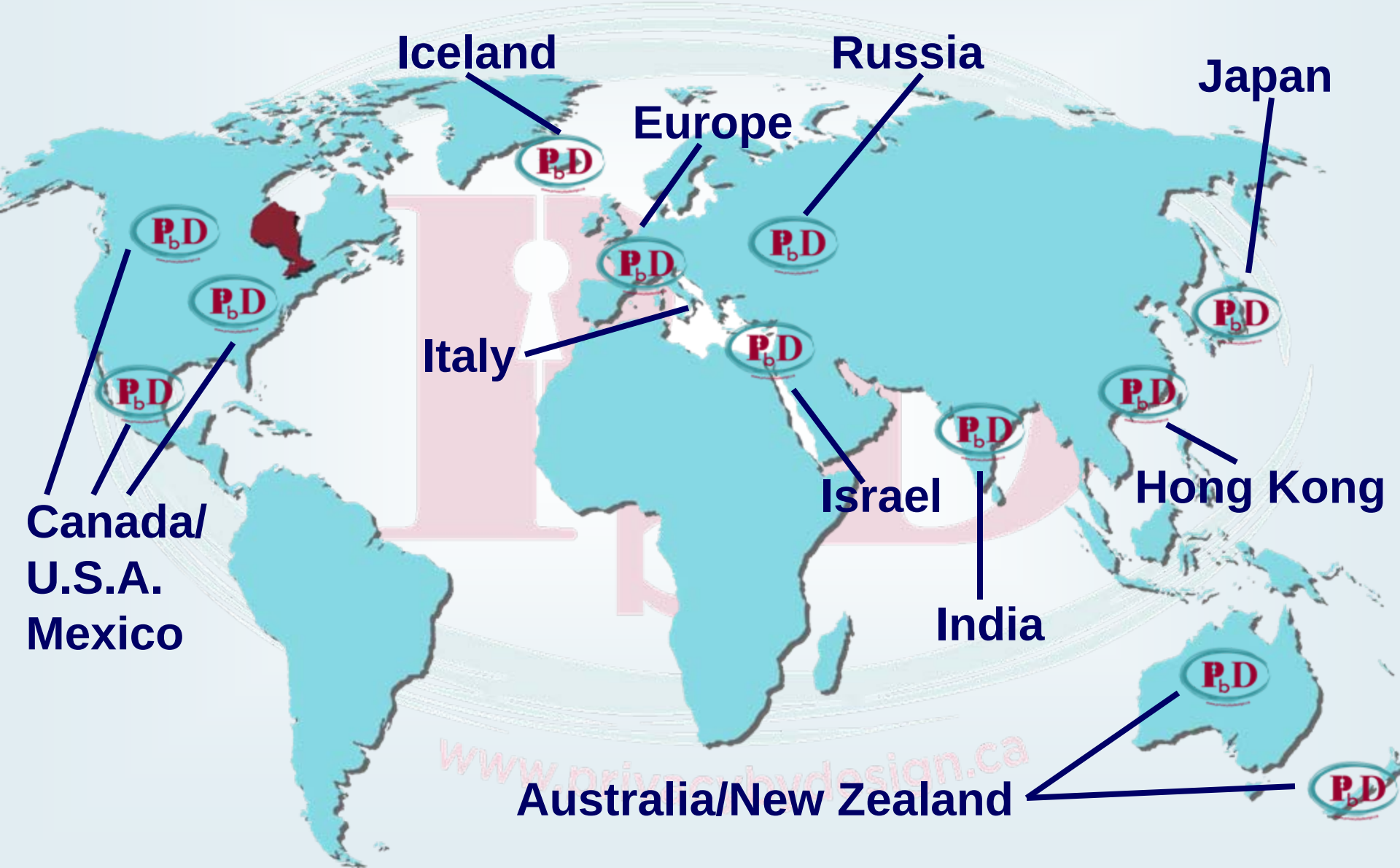
Adoption of "Privacy by Design" Resolution

- **October 29, 2010 –** regulators from around the world gathered at the annual assembly of International Data Protection and Privacy Commissioners in Jerusalem, Israel, and unanimously passed a landmark resolution recognizing *Privacy by Design* as an essential component of fundamental privacy protection:
  - Encourage the adoption of the principles of *PbD* as part of an organization's **default** mode of operation;
  - Invite Data Protection and Privacy Commissioners to promote *PbD*, foster the incorporation if its *7 Foundational Principles* in privacy policy and legislation in their respective jurisdictions, and encourage research into *PbD*.

Embedding Privacy at the Design Stage: *The Obvious Route*

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

Privacy by Design – "Going Viral"



Embedding *Privacy by Design* into Regulatory Structures

- While governments will continue to set the norms and standards, they should also adopt a more **proactive approach** by compelling the requirements of *Privacy by Design* (PbD) on the part of both public and private institutions;
- We will benefit enormously by **incorporating PbD into our regulatory structures**, thereby transforming a traditionally reactive instrument into one that instils proactive requirements.

Examples of Embedding *PbD* into Laws and Regulatory Structures

- Instantiating proactive privacy values in legislators, judges, lawyers, and legal staff;
- Initiating *PbD* in the legislation process;
- Embedding *PbD* in the processes of legal departments;
- Establishing a tradition of proactive *PbD* considerations for the drafting of new laws by legislation counsel;
- Embrace *PbD* principles to establish familiar language and clauses to be used by legislative counsel, to express routinely identified privacy issues for drafting new laws and regulations.

Smart Grid Privacy: Privacy by Design in Action

Smart Grid:
"Bigger than the Internet"

"Our expectation is that this network will be 100 or 1,000 times larger than the Internet. If you think about it, some homes have Internet access, but some don't. Everyone has electricity access – all of those homes could potentially be connected."

— Marie Hattar,

V.P. Cisco Network Systems Solutions,

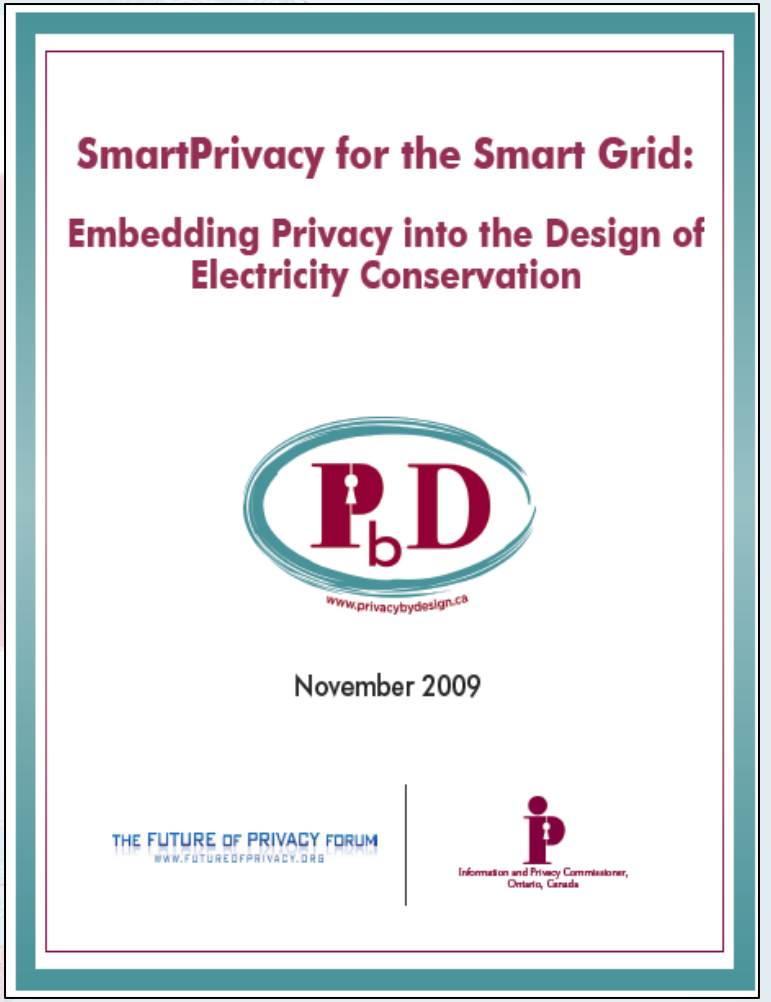
Cisco: Smart grid will eclipse size of Internet, CNET news.

http://news.cnet.com/8301-11128_3-10241102-54.html

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

Smart Grid Privacy

Privacy by Design:

Achieving the Gold Standard in Data Protection for the Smart Grid

June 2010

PbD
www.privacybydesign.ca

hydro one | Information & Privacy Commissioner of Ontario | toronto hydro corporation

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

"Assets Beyond the Meter — Who Should Own Them?"

"There are sound reasons why energy consumers should remain in control of the energy consumption information they produce, even if there isn't a law that requires this. The underlying rationale is that consumer confidence and trust in the Smart Grid, and in one's local electricity distributors, is ***vital*** *in achieving the vision of a more energy efficient electrical grid."*

— Commissioner Cavoukian,
Electric Light & Power Magazine
www.elp.com

Addressing Challenges

- Utilities will find opportunities to adopt ***Privacy by Design*** when introducing new technologies into the development of the Smart Grid, integrating communications, operational and information systems, as well as updating business processes.

Best practices for Smart Grid
Privacy by Design

1. Smart Grid systems should feature privacy principles in their overall project governance framework and **proactively** embed privacy requirements into their designs, in order to **prevent** privacy-invasive events from occurring – prevent the harm from arising;
2. Smart Grid systems must ensure that privacy is embedded as the default – the "no action required" automatic mode of protecting consumers' privacy – its presence must be ensured;

Best practices for Smart Grid
Privacy by Design (Cont'd)

3. Privacy must be made a core functionality in the design and architecture of Smart Grid systems and practices – an essential design feature;

4. Smart Grid systems must avoid unnecessary, zero-sum trade-offs between privacy and legitimate objectives of Smart Grid projects – adopt a positive-sum paradigm;

5. Smart Grid systems must build in privacy end-to-end, throughout the entire life cycle of any personal information collected;

Best practices for Smart Grid
Privacy by Design (Cont'd)

6. Smart Grid systems must be visible and transparent to consumers – engaging in accountable business practices – ensuring that new systems operate according to open, stated objectives;
7. Smart Grid systems must be designed with respect for consumer privacy, ***as a core foundational requirement***, to enhance consumer confidence and trust.

Use Case Scenario for

Smart Grid *Privacy by Design:*

Customer Enablement

Customer Enablement covers the end-to-end scope of a customer's interaction with a utility's technology systems and processes involving three basic activities:

1. **Enrollment:** The ability for eligible customers to enroll and define their participation in programs offered by the utility;
2. **Usage (Operation):** The active operation and management of participating customers. This refers to the daily functioning of systems and processes for a utility to deliver the service;
3. **Termination:** The ability for customers to freely terminate their active participation – freedom of choice.

Use Case Scenario:

Details Relating to Usage

- A demand response system must determine how many consumer thermostats need to be adjusted;
- The system retrieves thermostat device information from the registration system, limiting the information retrieved to device identifier and user preferences (e.g. maximum/minimum temperature);
- The system collects ***no*** consumer data (e.g. name, telephone number, addresses, etc);
- Personally identifiable information is only needed for program enrolment, which operates separately from device management.

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

The Min/Max Principle

Use the *minimum* amount of
personal information
to achieve the *maximum* functionality

RESULT:
Data Minimization *and*
Achievement of Stated Objectives

WIN/WIN

SmartGrid Research Data Warehouse

- In September 2010, I 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;
- My office will play an advisory role based on our working relationship with Ontario's advanced metering infrastructure and expertise 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 (January, 2011).

Conclusions

- **Lead with *Privacy by Design;***
- **Time to change the paradigm from the dated "zero-sum" to the doubly-enabling "positive-sum;"**
- **Deliver *both* privacy AND security or any other functionalities, in an empowering "win-win" paradigm;**
- **Embed privacy as a core functionality: the future of privacy may depend on it!**

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