Build it into the System – Embed Privacy, by Design: A Call to Action

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

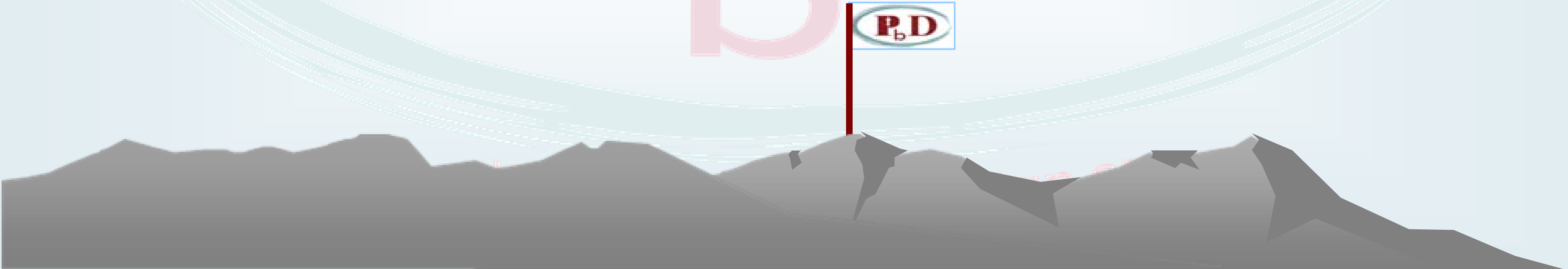
Ontario, Canada

Adobe
San Jose, California
May 12, 2011

Presentation Outline

1. *Privacy Landscape – Setting the Stage*
2. *We Need to Change the Paradigm*
3. *Privacy in the Clouds*
4. *PbD in Practice:*
    i. *Biometric Encryption*
    ii. *Smart Grid*
    iii. *Mobile Devices*
5. *Privacy by Design: The Gold Standard*
6. *Add Privacy – Gain a Competitive Advantage*
7. *Conclusions*

The Privacy Landscape



What is Privacy?

A fundamental human right –
– the basis of freedom and liberty.

Privacy = Freedom

Information Privacy Defined

Freedom of choice – personal control

“Informational self-determination”

Fair Information Practices (FIPs)

Global Privacy Standard (2006)

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

First Question to Ask:
Is it PII?

Is it Personally Identifiable Information?

FIPs: The Basics

Purpose Specification:

- *Identify the primary purpose – then only collect what you need;*
- *Data minimization – Minimize the collection of PII;*

Use Limitation:

- *Secondary purposes – don’t use the information collected for other secondary purposes, without the consent of the data subject;*

If you need a shorthand for thinking about privacy, think

“Use.”

OECD Fair Information Practices Principles

1. *Collection Limitation*
2. *Data Quality/Accuracy*
3. *Purpose Specification*
4. *Use Limitation*
5. *Security Safeguards*
6. *Openness/Transparency*
7. *Individual Participation*
8. *Accountability*

What Privacy is Not

Security ≠ Privacy

Security is, however, vital to privacy:
You cannot have Privacy without Security

Setting the Stage:

Why We Need to Change the Paradigm

Game Theory

Positive-Sum

Zero-Sum

Negative-Sum

The Future of Privacy

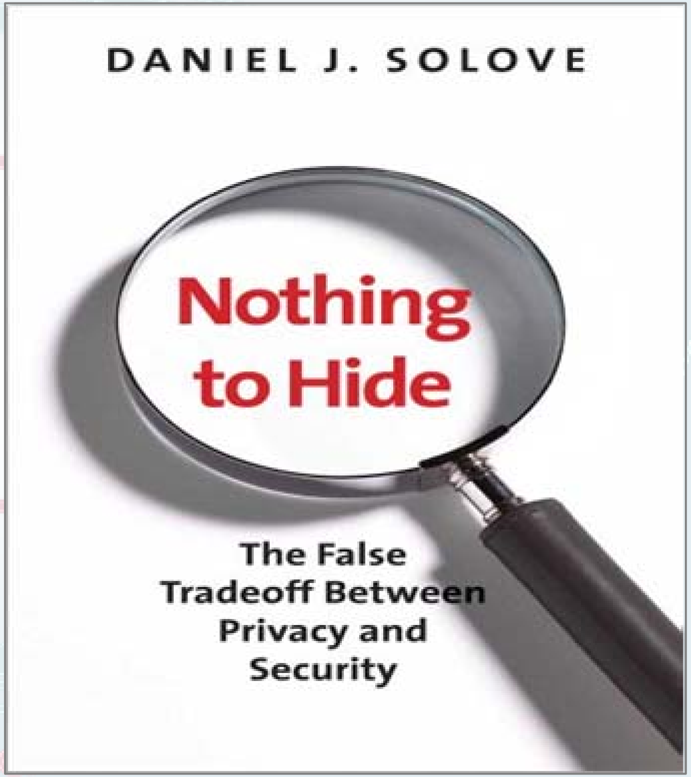
Change the Paradigm to Positive-Sum,

NOT

Zero-Sum

Nothing to Hide: The False Tradeoff between Privacy and Security

"The debate between privacy and security has been framed incorrectly as a zero-sum game in which we are forced to choose between one value and the other. Why can't we have both?"



DANIEL J. SOLOVE

Nothing to Hide

The False Tradeoff Between Privacy and Security

http://docs.law.gwu.edu/facweb/dsolove/

Technology is Not Enough?

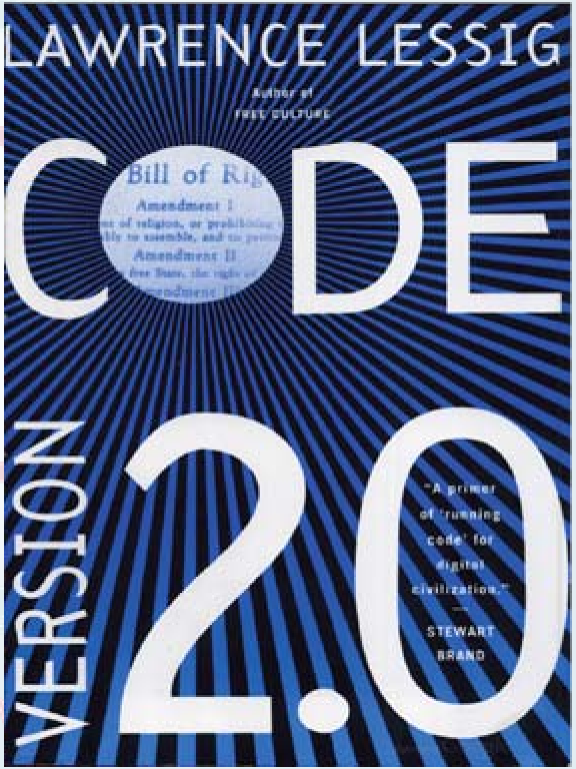
" … maybe we need to rely on policy and business practices and even legal constraints to protect people’s privacy, because technology is not necessarily adequate to do that.”

— Dr. Vint Cerf,
Stanford School of Engineering,
February 8, 2011.

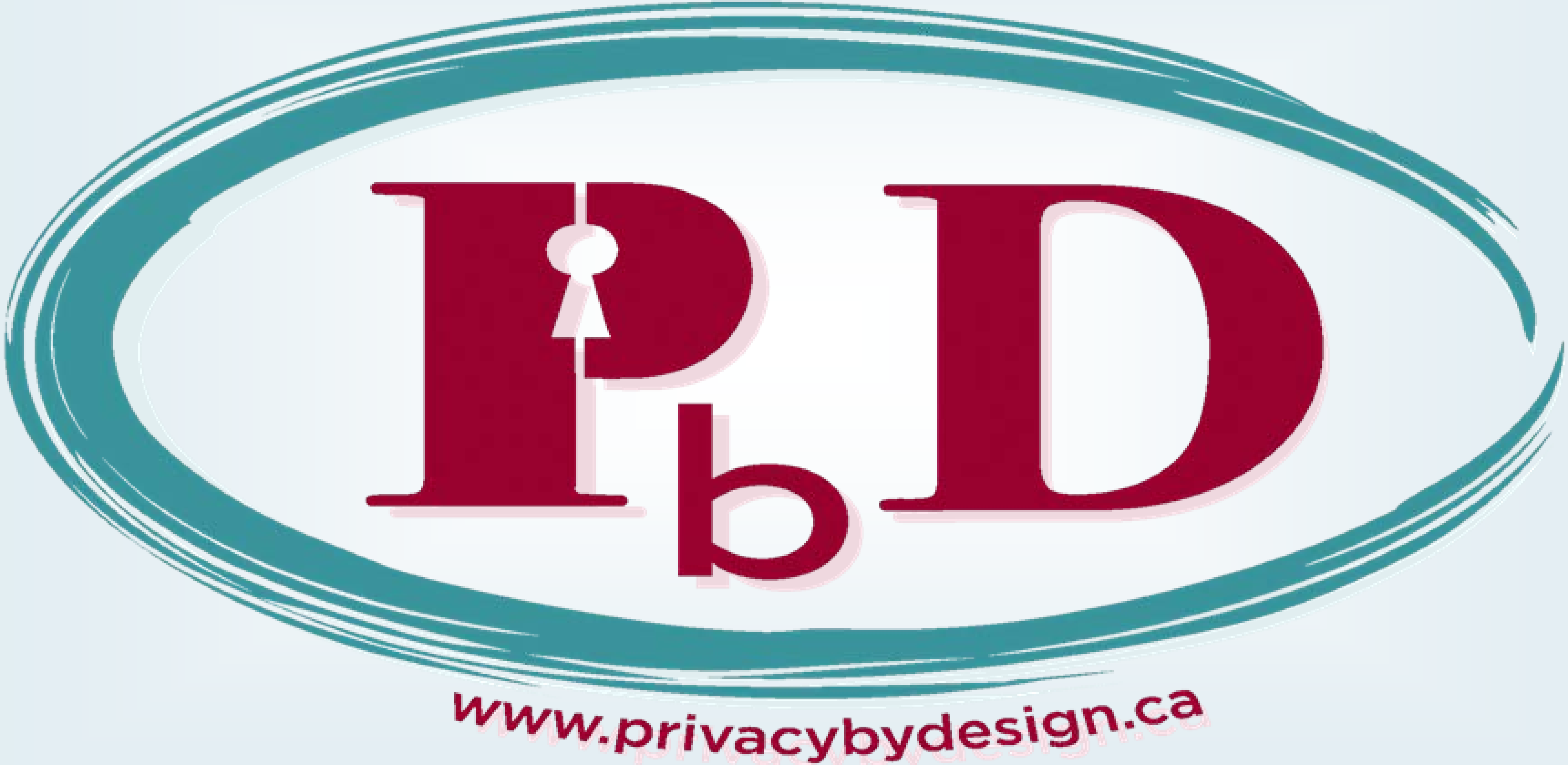
Marriage of Technology and Policy – Translate the Rules into Code

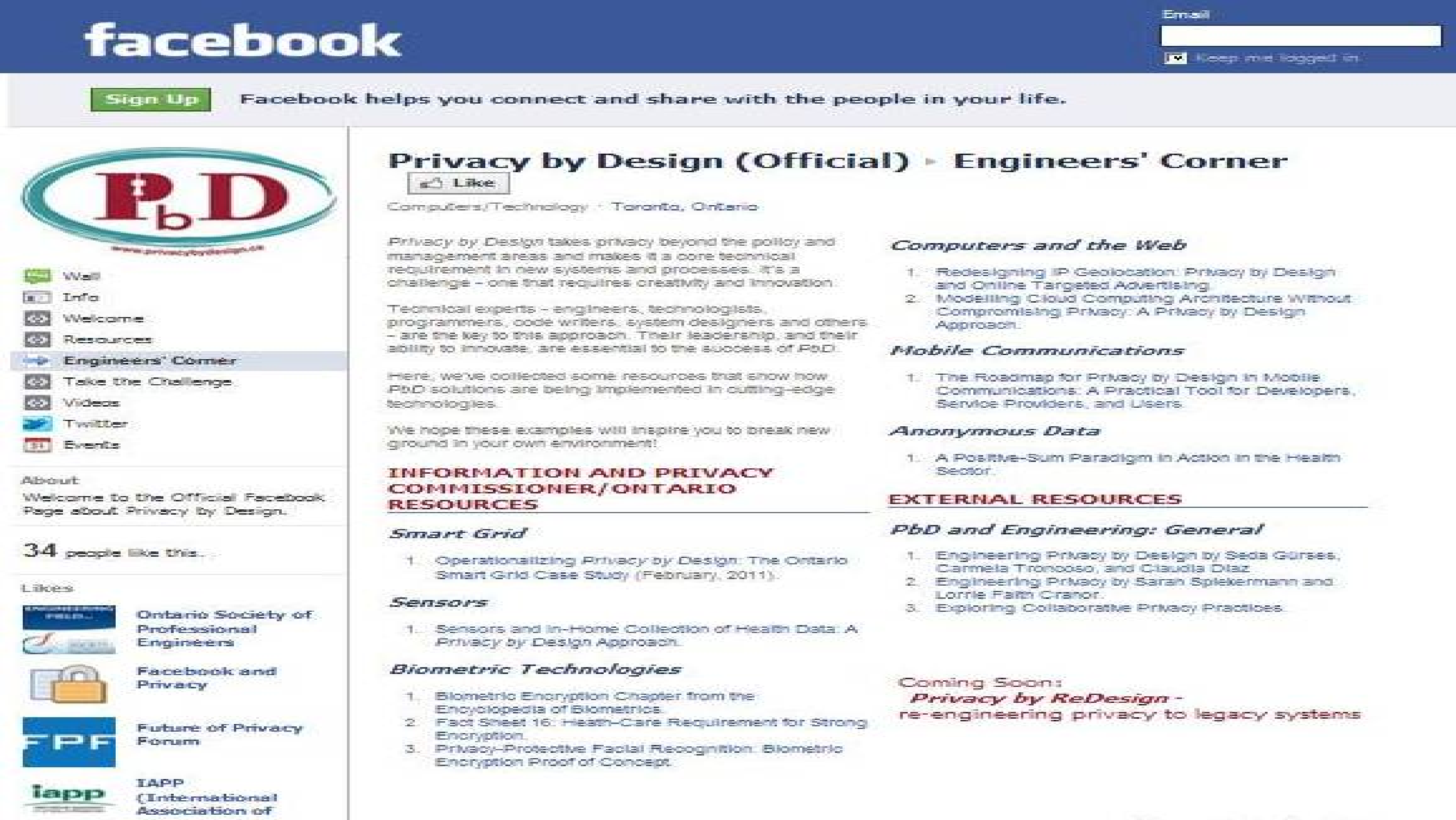
“A technology should reveal no more information than is necessary… it should be built to be the least revealing system possible.”

— Professor Lawrence Lessig,
Stanford Law School



A Decade of Privacy by Design





About

Welcome to the Official Facebook Page about Privacy by Design.

34 people like this.

Privacy by Design (Official) ▸ Engineers' Corner

Computers/Technology · Toronto, Ontario

Privacy by Design takes privacy beyond the policy and management areas and makes it a core technical requirement in new systems and processes. It's a challenge – one that requires creativity and innovation.

Technical experts – engineers, technologists, programmers, code writers, system designers and others – are the key to this approach. Their leadership, and their ability to innovate, are essential to the success of *PbD*.

Here, we've collected some resources that show how *PbD* solutions are being implemented in cutting-edge technologies.

We hope these examples will inspire you to break new ground in your own environment!

INFORMATION AND PRIVACY COMMISSIONER/ONTARIO RESOURCES

Smart Grid

1. Operationalizing *Privacy by Design*: The Ontario Smart Grid Case Study (February, 2011).

Sensors

1. Sensors and In-Home Collection of Health Data: A *Privacy by Design* Approach.

Biometric Technologies

1. Biometric Encryption Chapter from the Encyclopedia of Biometrics.
2. Fact Sheet 16: Health-Care Requirement for Strong Encryption.
3. Privacy-Protective Facial Recognition: Biometric Encryption Proof of Concept.

Computers and the Web

1. Redesigning IP Geolocation: Privacy by Design and Online Targeted Advertising.
2. Modelling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach.

Mobile Communications

1. The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users.

Anonymous Data

1. A Positive-Sum Paradigm in Action in the Health Sector.

EXTERNAL RESOURCES

PbD and Engineering: General

1. Engineering Privacy by Design by Seda Gürses, Carmela Troncoso, and Claudia Diaz
2. Engineering Privacy by Sarah Spiekermann and Lorrie Faith Cranor.
3. Exploring Collaborative Privacy Practices.

Coming Soon:
Privacy by ReDesign -
re-engineering privacy to legacy systems

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

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

The future of Privacy rests on creativity, innovation and collaboration

Privacy by Design and the Internet Engineering Task Force (IETF)

*“The concept of **Privacy by Design** has gotten a lot of attention over the past few years and within the IETF we have tried to investigate how we can consider privacy in the design of protocols and architectures in a more systematic way … in protocols and architectural designs.”*

“We have started to shed more light on privacy in the IETF by organizing a privacy workshop to solicit input from the technically minded privacy community, to create an IETF privacy directorate, and to start the work on a number of documents to offer more guidance to engineers.”

— *Privacy Considerations for Internet Protocols,*
Internet Engineering Task Force (IETF), www.ietf.org

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

IPSI

Engineering – Mathematics –
Computer Sciences – Information Studies

www.ipsi.utoronto.ca

Ryerson University

Digital Media Zone (DMZ) *is a place where students, alumni, and companies can turn their innovations into market-ready products while seeking solutions to real-world, real-time problems*

DMZ’s Flybits:
The Embodiment of PbD

- **Flybits** is a research team based at DMZ that focuses on ubiquitous and pervasive computing, with the goal of using mobile devices to enhance interpersonal communications, ***while conserving privacy;***

- The ambient intelligence required for successful context-aware applications gives Flybits a mandate to develop ***solutions for unique privacy problems***;

- Flybits is leading a project focused on building a **Privacy Rule Engine** for preserving user privacy in ubiquitous software applications.

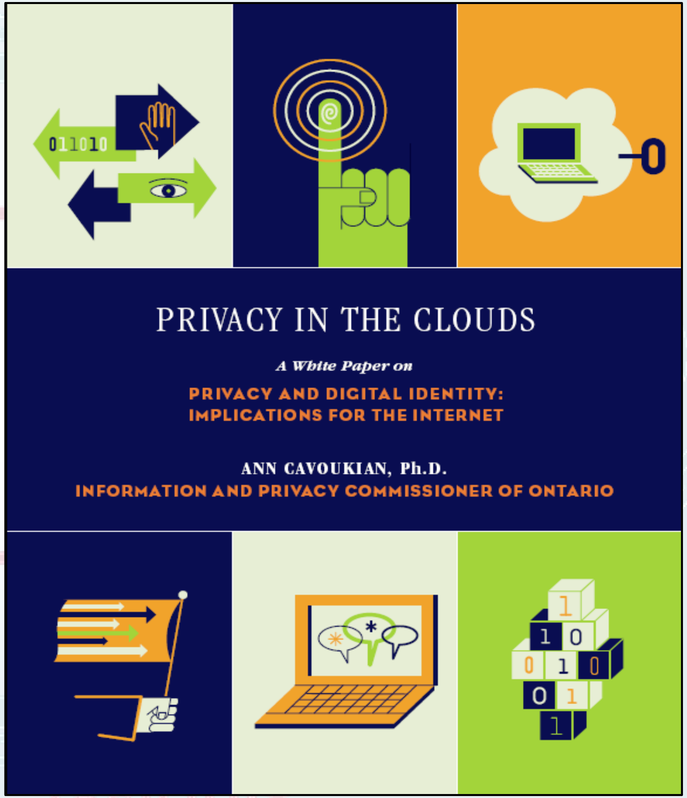
http://digitalmediazone.ryerson.ca/tag/flybits/

Privacy by Design Meets the Cloud

- There is both the need and opportunity to engineer privacy, security and trust directly into new emergent Internet and web architectures:
  - Interoperable identity metasystems;
  - Cloud-based services, platforms and infrastructures;
  - The “Internet of Things;”
  - The programmable web, or “WebOS.”

Privacy in the Clouds

- The 21st Century Privacy Challenge;
- Creating a User-Centric Identity Management Infrastructure;
- Using Information Technology Building Blocks;
- A Call to Action!



PRIVACY IN THE CLOUDS

A White Paper on

PRIVACY AND DIGITAL IDENTITY: IMPLICATIONS FOR THE INTERNET

ANN CAVOUKIAN, Ph.D.
INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

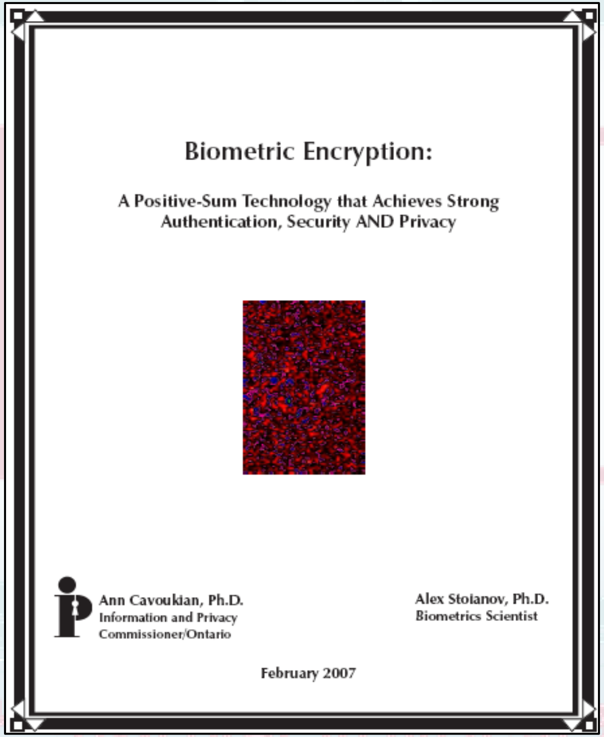
www.ipc.on.ca/images/Resources%5Cprivacyintheclouds.pdf

Privacy by Design Meets the Cloud: Current and Future Privacy Challenges

- Collaborating together to build innovative win-win privacy solutions;

- The goal is to establish ***trust*** in various platforms:
  - All data (that travels through the cloud);
  - Personal and mobile devices (that interact with cloud-based services);
  - Intelligent software agents;
  - Intermediary service providers.

Biometric Encryption:
A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy



Biometric Encryption:

A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy

Ann Cavoukian, Ph.D.
Information and Privacy
Commissioner/Ontario

Alex Stoianov, Ph.D.
Biometrics Scientist

February 2007

www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf

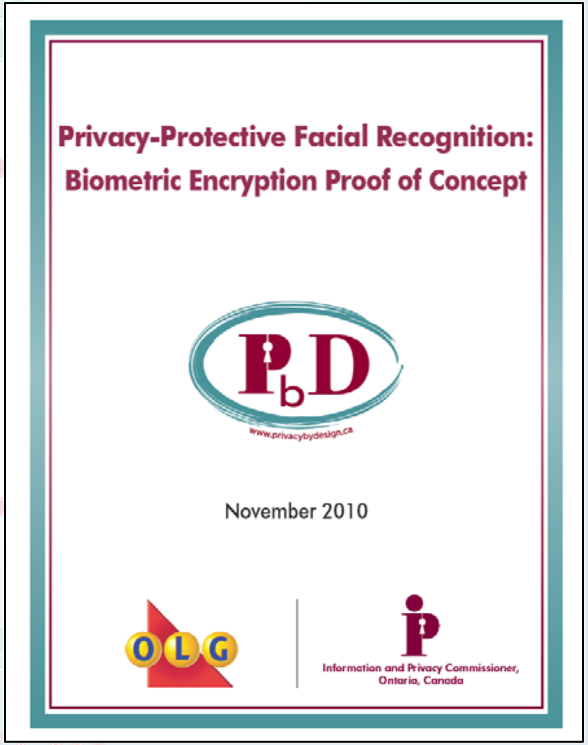
Biometric Encryption

- Privacy-enhanced uses of biometrics, with a particular focus on the privacy and security advantages of BE, over other biometrics;

- How BE technology can overcome the prevailing “zero-sum” paradigm by effectively transforming one’s biometric into a private key.

Biometric Encryption:
The Privacy by Design Approach

“The rapid, accurate identification and authentication of individuals has become a challenge across many sectors and jurisdictions … Increasingly, biometric encryption is being viewed as the ultimate means of authentication or identification across a broad range of applications.”



Privacy-Protective Facial Recognition:
Biometric Encryption Proof of Concept

www.privacybydesign.ca

November 2010

Information and Privacy Commissioner,
Ontario, Canada

www.privacybydesign.ca

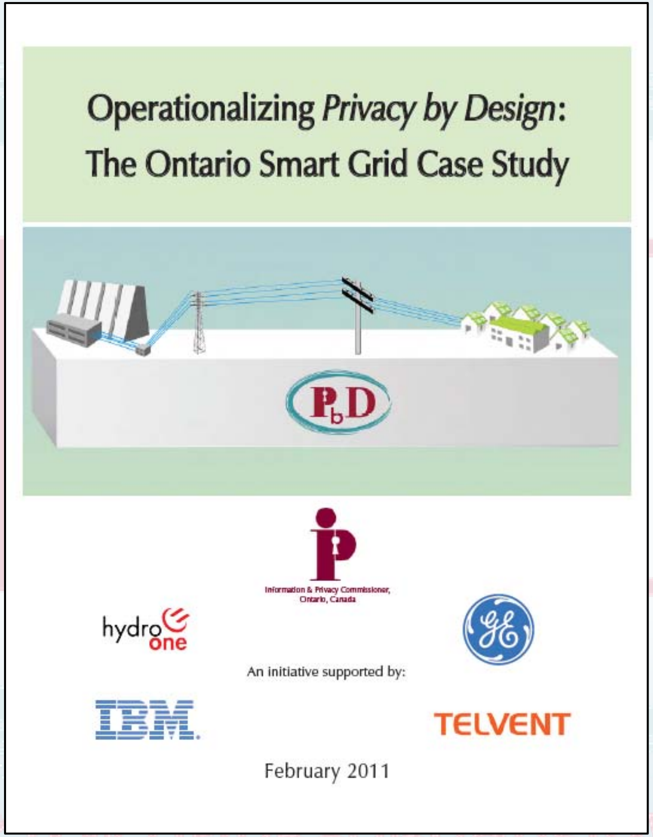
OLG Self-Exclusion program

- Totally voluntary self-excluded individuals – more than 12,000 in Ontario and growing – who want to be kept out of casinos;
- **Great need** for reliable detection of those attempting to enter a gaming site – manual comparison alone does not work;
- Privacy of ***all*** casino patrons must be protected;
- **Solution:** Facial recognition with the use of *Biometric Encryption*;
- Novel ***"Made in Ontario"*** PbD application: collaboration of OLG, IPC, UofT, and iView Systems.

Facial Recognition with Biometric Encryption

- ***Biometric Encryption*** (BE): securely binds a person’s identifier (pointer to personal information) with facial biometrics;
- The pointer is retrieved only if a correct (i.e., self-excluded) person is present;
- The link between facial templates and personal information is controlled by BE;
- Final comparison is done manually;
- No biometric template is ever retained in the database;
- Privacy of both the public ***and*** self-excluded individuals is protected.

Operationalizing *Privacy by Design* into the Smart Grid:



Operationalizing *Privacy by Design*:
The Ontario Smart Grid Case Study

Information & Privacy Commissioner,
Ontario, Canada

An initiative supported by:

February 2011

www.privacybydesign.ca

Operationalizing *Privacy by Design* (Cont'd)

- Methodology for Operationalization of *PbD*;
- Operationalizing *Privacy by Design* across Smart Grid Domains;
- Working with partners – Hydro One, GE, IBM, Telvent.

"Make privacy an element of the architecture – a key non-functional attribute"

— Austin Montgomery,
Software Engineering Institute,
Carnegie Mellon University

Translate business goals into the system's architecture

Smart Grid Maturity Model

The Smart Grid Maturity Model (SGMM)

- The SGMM is a management tool that provides a common framework for defining key elements of Grid transformation, and helps utilities develop, track, and plan their progress;
- The SGMM defines maturity levels, sets of qualitative characteristics that indicate increasing maturity levels in 8 domains of Smart Grid development;
- Privacy is a key non-functional quality attribute.

Mobile/Smartphone Tracking Debate

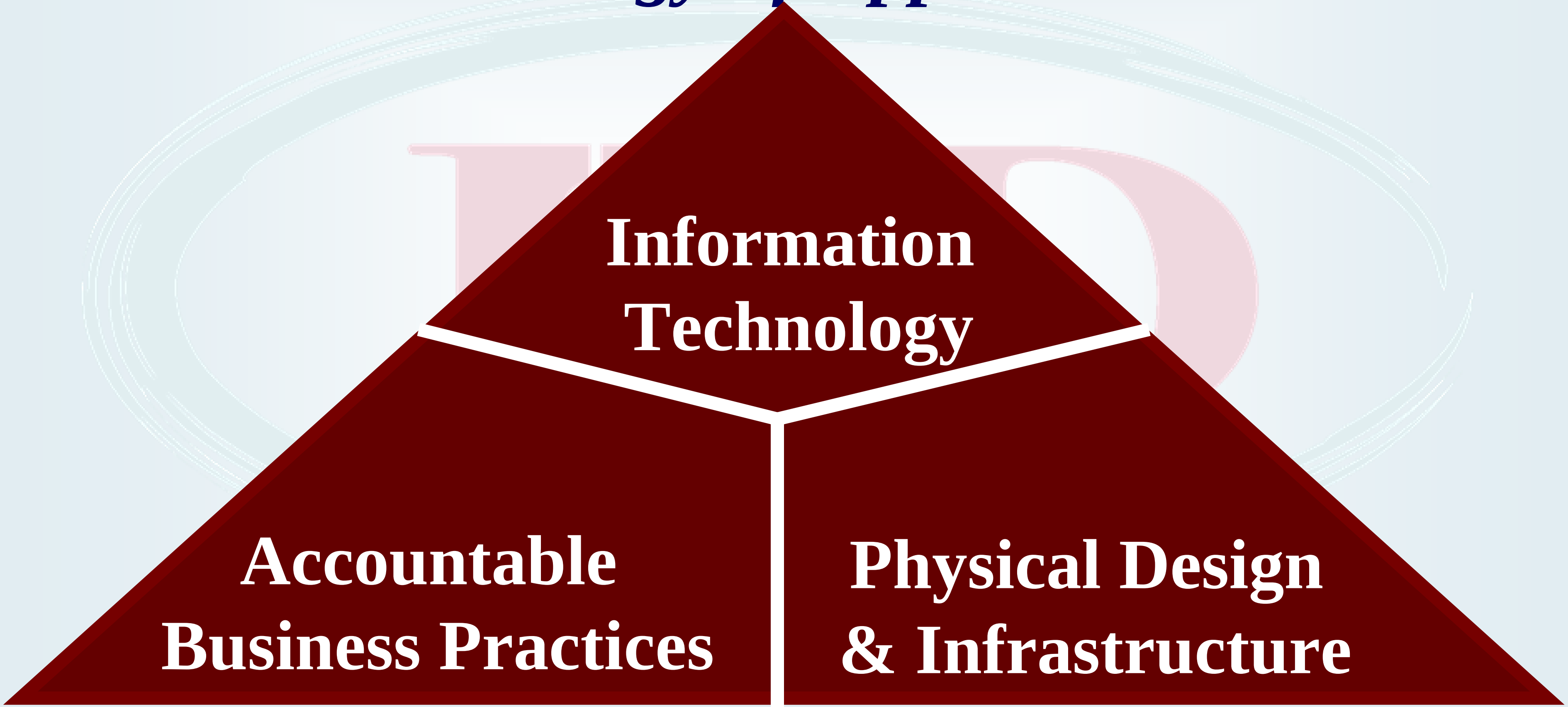
- **Transparency** – give users clear notification from the outset;
- **Consent** – make it user-centric – make privacy the default;
- **Anonymized data** – don't let it be linked back to identifiers;
- **Data Minimization** – don’t collect more data than you need;
  - When consumers find out *after the fact* that their data is being tracked, it erodes confidence and trust;
  - This is why we need *Privacy by Design* – privacy controls embedded directly into the system, right from the outset … otherwise you can end up with *Privacy by Disaster*.

What is Privacy by Design?

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



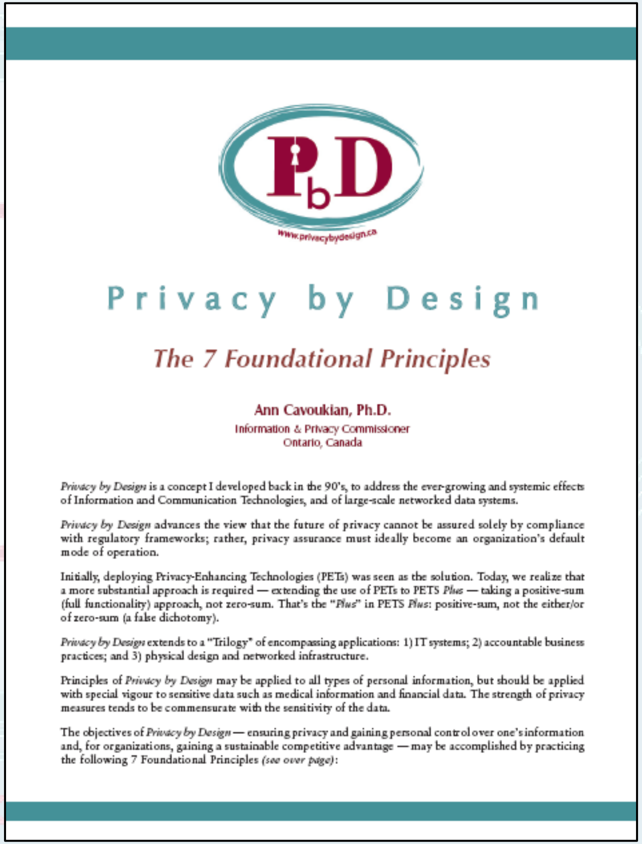
Information Technology

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*** setting;
3. Privacy ***Embedded*** into Design;
4. ***Full*** Functionality:
   Positive-Sum, not Zero-Sum;
5. End-to-End **Security**:
   Full Lifecycle Protection;
6. Visibility **and** Transparency:
   Keep it Open;
7. Respect for User Privacy:
   Keep it User-Centric.



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:
Proactive in 21 Languages!

1.English

2.French

3.German

4.Italian

5.Spanish

6.Czech

7.Dutch

8.Estonian

9.Hebrew

10.Hindi

11.Chinese

12.Japanese

13.Arabic

14.Armenian

15.Korean

16.Ukrainian

17.Russian

18.Romanian

19.Portuguese

20.Maltese

21.Greek

The Bottom Line

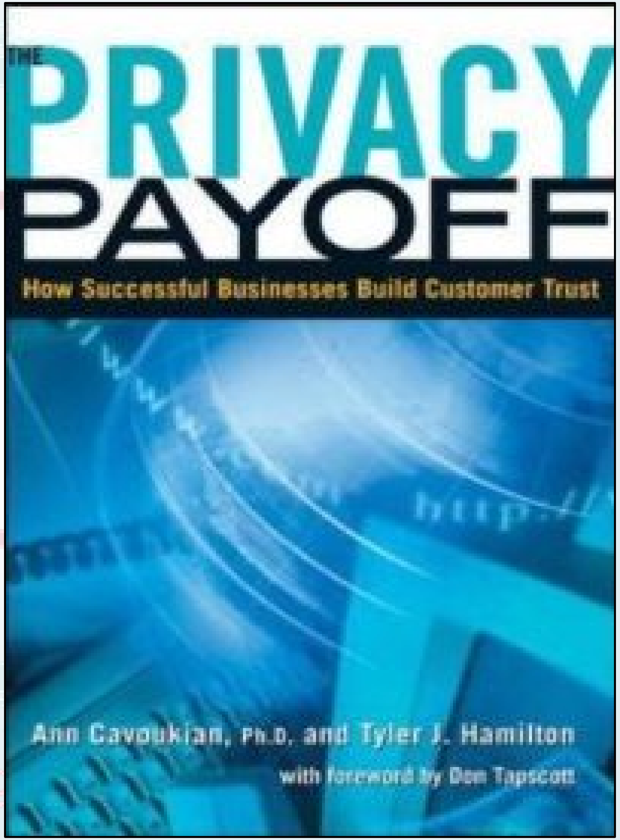
Privacy should be viewed as a **business** issue, not a ***compliance*** issue

Think strategically and transform privacy into a competitive business advantage

Privacy is *Good* for Business

- Facilitates continuation of valuable business relationships;
- Serves to preserve existing customers, and attract new ones;
- Fosters the development of a sustainable competitive advantage;
- Builds consumer confidence and trust.

— Ann Cavoukian, Ph.D., Tyler Hamilton,
The Privacy Payoff: How Successful Businesses Build Consumer Trust, McGraw-Hill Ryerson, 2002.


THE
PRIVACY
PAYOFF
How Successful Businesses Build Customer Trust
http://
Ann Cavoukian, Ph.D. and Tyler J. Hamilton
with foreword by Don Tapscott

Cost of Taking a Reactive Approach to Privacy Breaches

Proactive

Lawsuits

Damage to Brand and Reputation

Reactive

Loss of Consumer Confidence and Trust

Consumer Choice and Privacy
It’s All About Trust

- There is a strong competitive advantage for businesses to invest in good data privacy and security practices;

“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

Conclusions

- This is a Call to Action – we need your help;
- Lead with *Privacy by Design*, and gain a competitive advantage;
- Change the paradigm from the dated “zero-sum” to the doubly-enabling “positive-sum;”
- Deliver *both* privacy AND *(not vs.)* any other functionality, in an empowering “win-win” paradigm – abandon false trade-offs;
- Creativity and innovation are essential to win the day!
- Embed privacy as a core functionality: the future of privacy (and freedom) 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