

***Build it Right 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***

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



**Privacy = Freedom**

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

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

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

# 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*

**For Shorthand Privacy: Think “Use”**

# Survey Results are in:

## *Consumers Say Privacy is a Bigger Concern than Security on Smartphones*

- **Privacy concerns rank #1:** Most consumers expressed great concern about their data privacy, both when using smartphones in general, and when using mobile apps in particular;
- Consumers want more control over their data: **98%** of consumers expressed a strong desire for better controls over how their personal information is collected and used via mobile devices and apps;
- A significant majority (**77%**) of consumers don't want to share their location data with app owners/developers.

# Mobile/Smartphone Tracking

- **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*.



***We Need to  
Change the Paradigm***

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

# The Future of Privacy:

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

*Proactively embed the necessary protections directly into the system*

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

# 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.

# *A Decade of Privacy by Design*



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

***The future of Privacy rests on  
creativity, innovation  
and collaboration***

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

# *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](http://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**

The logo for the Identity, Privacy and Security Institute (IPSI) features the acronym 'IPSI' in a bold, green, serif font. The letters are set against a white rectangular background. This background is centered within a larger, light blue oval shape that has a subtle, multi-layered border. Behind the white rectangle, there is a faint, large-scale watermark of the letters 'IPSI' in a reddish-pink color.

**Engineering – Mathematics –  
Computer Sciences – Information Studies**

**[www.ipsi.utoronto.ca](http://www.ipsi.utoronto.ca)**

[Sign Up](#)

Facebook helps you connect and share with the people in your life.



- Wall
- Info
- Welcome
- Resources
- Engineers' Corner**
- Take the Challenge
- Videos
- Twitter
- Events

**About**

Welcome to the Official Facebook Page about Privacy by Design.

35 people like this.

**Likes**

- Future of Privacy Forum**
- Ontario Society of Professional Engineers**
- Facebook and Privacy**
- IAPP (International Association of Privacy Professionals)**

**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 Design* by Sarah Spiekermann and Lorrie Faith Cranor.
3. Exploring Collaborative *Privacy* Practices.

Coming Soon:

***Privacy by ReDesign*** - Re-engineering privacy to existing legacy systems

# Ryerson University

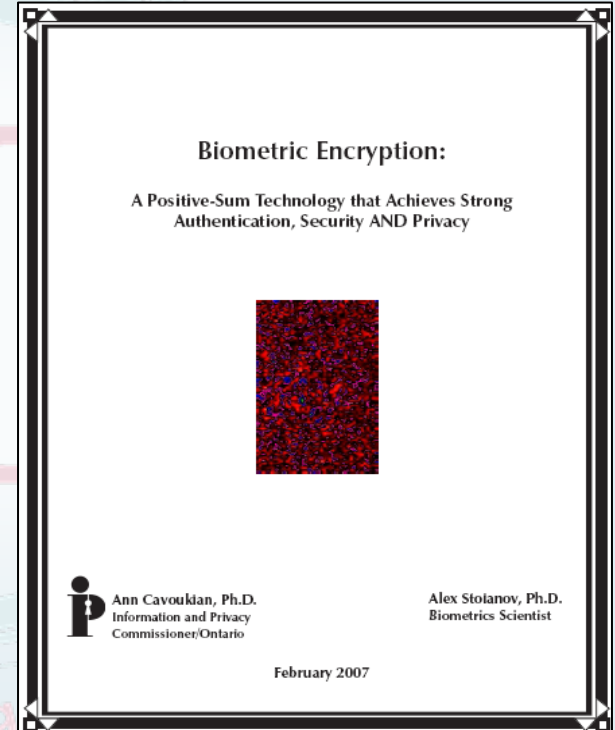
*Digital Media Zone (DMZ) is a place where students, alumni, and companies can turn their innovations into market-ready products while seeking solutions to real-world, real-time problems*

**Flybits** – 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;*

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

## Existing Applications:

- Video Surveillance cameras on mass transit system;
- Casinos and gaming facilities.



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

[www.ipc.on.ca/images/Resources/up-1bio\\_encryp.pdf](http://www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf)

# Casino 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 *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;
- Additional, 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:

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



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

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

***“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***

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



*What is  
Privacy by Design?*

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

# *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.



# 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 ...  
replace “vs.” with “and”*

# *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

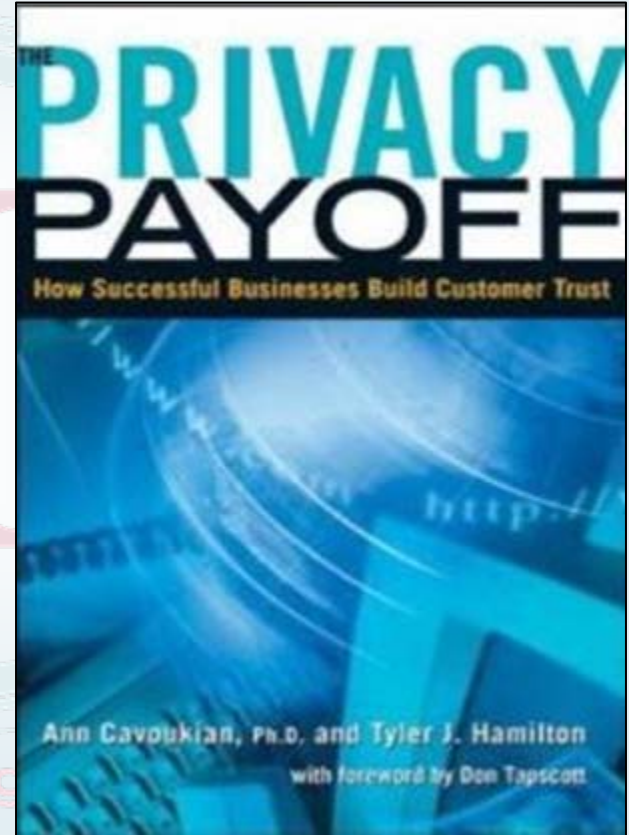
Privacy should be viewed as a  
**business** issue, not a  
*compliance* issue

*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.



# *Cost of Taking a Reactive Approach to Privacy Breaches*

**Proactive**



**Lawsuits**

**Damage to Brand  
and Reputation**

**Reactive**



**Loss of Consumer Confidence  
and Trust**

# 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.**

[www.ipc.on.ca/english/Resources/Presentations-and-Speeches/](http://www.ipc.on.ca/english/Resources/Presentations-and-Speeches/)

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

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

**For more information on *Privacy by Design*, please visit:**

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