

*Get Smart About Privacy:
SmartPrivacy and Privacy by Design*

Ann Cavoukian, Ph.D.

**Information and Privacy Commissioner
Ontario**

**International Association of Privacy Professionals
KnowledgeNet 2009
*October 20, 2009***



Presentation Outline

- 1. The Privacy Landscape*
- 2. The Future of Privacy: Positive-Sum,
NOT Zero-Sum*
- 3. Get Smart About Privacy: SmartPrivacy*
- 4. The Next Wave: From PETs to PETs Plus,
... to Transformative Technologies*
- 5. RFID Transformed: Add an On/Off Device*
- 6. Smart Grid*
- 7. Conclusions*



The Privacy Landscape



What Privacy is Not

Privacy \neq Security

Security *is*, however, vital to privacy



*If privacy is to
live well into the future,
things have to change*



The Future of Privacy:

Positive-Sum

NOT

Zero-Sum



*We need to
change
the paradigm*



Positive-Sum Paradigm

- A **Zero-Sum Paradigm** describes a concept or situation in which one party's gains are balanced by another party's losses – win/lose; either/or; enhancing security often comes at the expense of privacy – the more you have of one, the less you can have of the other;
- A **Positive-Sum Paradigm**, in contrast, describes a situation in which *all* participants may mutually gain together (win-win);
- To achieve a positive-sum model, privacy must be proactively built into the system so that privacy protections are engineered directly into the technology, right from the outset;
- The effect is a minimization of the unnecessary collection and use of personal data by the system, while at the same time, strengthening data security, and empowering individuals to exercise greater control;
- This can result in technologies that achieve strong security *and* privacy, or privacy *and* functionality, delivering a “win-win” outcome.

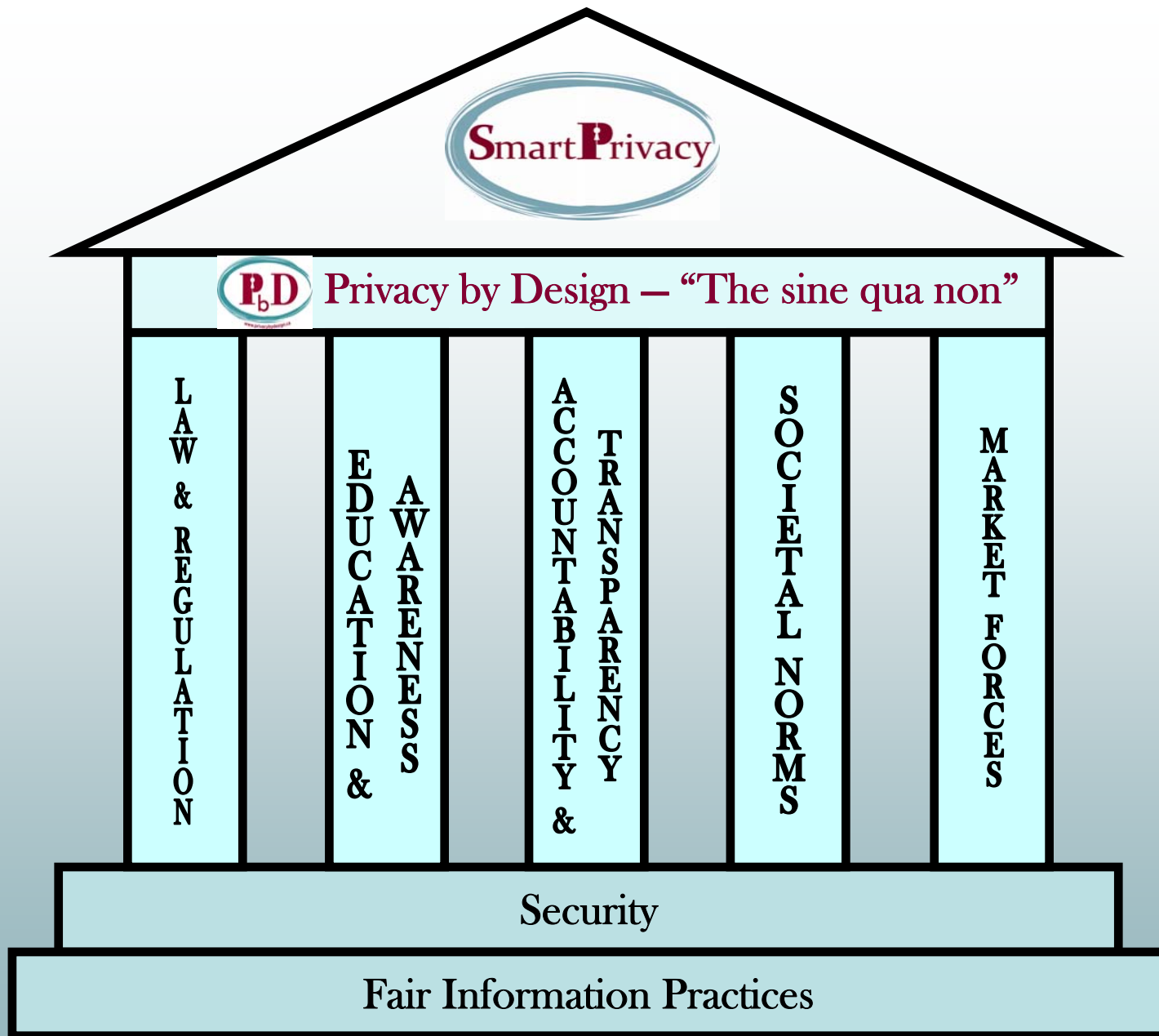


Positive-Sum Model

*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*



*Get Smart About Privacy:
“SmartPrivacy”*



“SmartPrivacy is the umbrella that offers the complete suite of protections to ensure data privacy. It consists of multiple measures ranging from regulatory protections to education and awareness, but one measure stands out as the sine qua non: *Privacy by Design*.
Dr. Ann Cavoukian, Information & Privacy Commissioner of Ontario.



www.privacybydesign.ca



Privacy by Design: “Build It In”

- I first developed the concept of “Privacy by Design” in the 90s, as a response to the growing threats to online privacy that were beginning to emerge;
- “Privacy by Design” seeks to build in privacy – up front, right into the design specifications; into the architecture; embed privacy into the technology used – *bake it in*;
- Data minimization is key: minimize the routine collection and use of personally identifiable information – use encrypted or coded information whenever possible;
- Use privacy-enhancing technologies (PETs) where possible: give people maximum control over their own data.



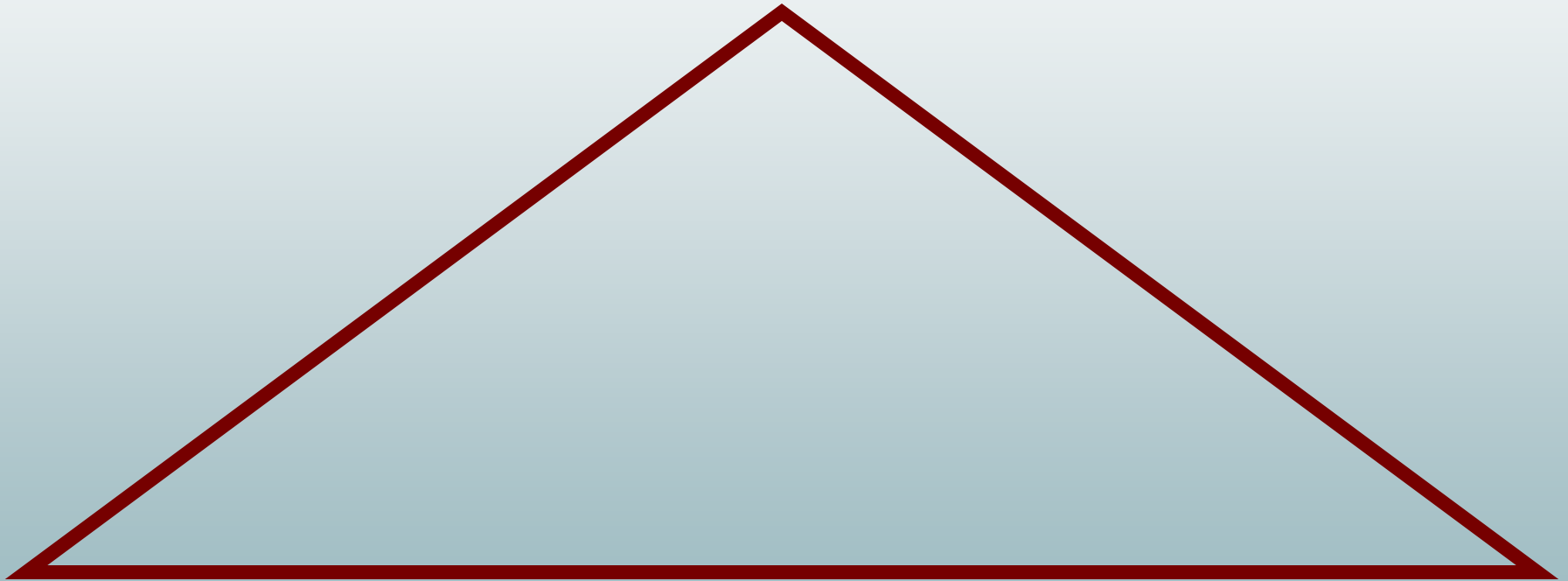
Why We Need *Privacy by Design*

- 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 a model for ensuring the future of privacy; for that, we must turn to measures such as *Privacy by Design: the Gold Standard*, – embedding privacy proactively into the core.



Privacy by Design: *The Trilogy of Applications*

Information Technology



**Accountable
Business Practices**

**Physical Design
& Infrastructure**




Privacy by Design: *Focus for 2009*

- **Technology** – Building privacy directly into technology, at the earliest developmental stage;
- **Accountable Business Practices** – Incorporating privacy into competitive business strategies and operations;
- **Physical Design and Infrastructure** – Ensuring privacy in health care settings and networked 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 Lifecycle Protection*
- 6. Visibility and Transparency*
- 7. Respect for User Privacy*


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 "Triology" 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.



The Next Wave:

From PETs to PETs Plus,

to

Trans Tech



Background:

Privacy-Enhancing Technologies (*PETs*)

- The IPC and the Dutch Data Protection Authority coined the concept and methodology recognized around the world today as *privacy-enhancing technologies* (PETs);
- In 1995, the IPC and the Dutch Data Protection Authority published their landmark study, *Privacy-Enhancing Technologies: The Path to Anonymity*.

Vol. I - www.ipc.on.ca/index.asp?layid=86&fid1=329

Vol. II - www.ipc.on.ca/images/Resources/anoni-v2.pdf



Time for a Change...

***... from PETs
to
PETs Plus***



PETs *Plus*

The “*Plus*” in PETs *Plus* refers to incorporating a positive-sum paradigm



Taking PETs *Plus* Further

from PETs Plus

to ...

Transformative Technologies



Transformative Technologies

**Privacy-Invasive Technology + Positive-Sum Paradigm +
Privacy-Enhancing Technology =
Transformative Technology**

Common characteristics of Transformative Technologies:

- Minimize the unnecessary collection, disclosure, use and retention of personal data;
- Empower individuals to participate in the management of their own personal data;
- Enhance the security of personal data, if collected/used;
- Promote public confidence and trust in personal data governance structures;
- Promote/facilitate the commercialization and adoption of these technologies.



Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum not Zero-Sum

- Examples of Transformative Techs if *PbD* enabled:
 - Biometric Encryption
 - RFID
 - Smart Grid

**Transformative Technologies Deliver
Both Security and Privacy:
Think Positive-Sum not Zero-Sum**

by
Ann Cavoukian, Ph.D.
Information and Privacy Commissioner
Ontario, Canada

Privacy, in the form of informational privacy, refers to an individual's ability to exercise personal control over the collection, use and disclosure of one's recorded information. Thus far, a "zero-sum" approach has prevailed over the relationship between surveillance technologies and privacy. A zero-sum paradigm describes a concept or situation in which one party's gains are balanced by another party's losses – win/lose. In a zero-sum paradigm, enhancing surveillance and security would necessarily come at the expense of privacy; conversely, adding user privacy controls would be viewed as detracting from system performance. I am deeply opposed to this viewpoint – that privacy must be viewed as an obstacle to achieving other technical objectives. Similarly, it is unacceptable for the privacy community to reject all forms of technology possessing any surveillance capacity and overlook their growing applications.

Rather than adopting a zero-sum approach, I believe that a "positive-sum" paradigm is both desirable and achievable, whereby adding privacy measures to surveillance systems need not weaken security or functionality but rather, could in fact enhance the overall design. A positive-sum (win-win) paradigm describes a situation in which participants may all gain or lose together, depending on the choices made.

To achieve a positive-sum model, privacy must be proactively built into the system (I have called this "privacy by design"), so that privacy protections are engineered directly into the technology, right from the outset. The effect is to minimize the unnecessary collection and uses of personal data by the system, strengthen data security, and empower individuals to exercise greater control over their own information. The result would be a technology that achieves strong security *and* privacy, with a "win-win" outcome.

By adopting a positive-sum paradigm and applying a privacy-enhancing technology to a surveillance technology, you develop, what I am now calling, "Transformative Technologies." Among other things, transformative technologies can literally transform technologies normally associated with surveillance into ones that are no longer privacy-invasive, serving to minimize the unnecessary collection, use and disclosure of personal data, and promoting public confidence and trust in data governance structures.

**Positive-Sum Paradigm + Privacy-Enhancing Technology
(applied to Surveillance Technology) = Transformative Technology**



RFID Transformed: On/Off Device



RFID Transformed: The Problem

- Privacy concerns arise when RFIDs are *associated with personally identifiable individuals*;
- Without appropriate security measures, embedding passive RFIDs into identity cards is problematic;
- The solution generally proposed – a protective sleeve, or Faraday Cage, is not sufficient.



The Problem (Cont'd)

- WHTI-compliant passcards and Enhanced Driver Licences (EDLs) contain passive RFID tags;
- These ID cards are being rolled out in border states and provinces, including Ontario;
- Our position: you should be able to turn the RFID off – the *default should be off* (the most privacy-protective option), unless the user chooses to turn it *on*, when needed.



RFID Transformed: The Solution

- We asked technology experts, *how can you turn it off?*
- Impinj® Inc., (www.impinj.com), has developed a prototype Gen2 RFID Tag (TouchTag™) that functions only when activated by human touch – at a distance of up to 30 feet (9 metres);
- The tag remains *inoperative* (off) until the user touches a specific spot on the tag, which then enables the tag to be read;
- When the user releases his or her finger from the tag, it once again becomes inoperative – it turns off (which becomes the default);
- * • **November 2, 2009** – Impinj® Inc. will be joining me in Madrid at the *Privacy by Design Workshop* where they will also have their RFID Tag technology on display – www.privacybydesign.ca/madrid09.htm



*SmartPrivacy for the
Smart Grid*



Smart Grid:

What is It?

- The smart grid refers to an electricity system that monitors and optimizes its interconnected elements (e.g., generators, high-voltage networks, energy storage installations, and end-use consumers including household appliances and devices);
- A smart meter is a meter that can record and report electricity consumption information automatically;
- In our jurisdiction, Ontario, old hydro meters read manually, are being replaced by smart meters.



Ontario's Smart Meter Initiative

- The Government of Ontario has committed to install a smart electricity meter in all homes and small businesses by the end of 2010 – *Energy Conservation Responsibility Act, 2006*;
- Smart meters will record electricity consumption on an hourly basis and report that information via a wireless technology;
- Individuals will be able to access their meter data from the previous day and be able to make choices about how to take advantage of future rates;
- A 'smart metering entity' (the Independent Electricity System Operator, or IESO) will receive and process the hourly consumer consumption data transmitted daily;
- The IESO is a listed institution under Ontario's *FIPPA*.



Smart Grid: *Privacy Risks*

- The information collected on a smart grid can form a library of personal information, the mishandling of which can lead to invasion of consumer privacy;
- An electricity usage profile can translate into a source of detailed behavioural information;
- Major concerns will arise if consumer-focused principles of transparency and control are not treated as essential design principles, from end to end.



Smart Grid:

Where the IPC stands

- While the smart grid is a good idea, the focus has almost exclusively been on controlling energy use, making privacy a sleeper issue. We must take care not to sacrifice consumer privacy amidst a sea of enthusiasm for electricity reform;
- Principles of *Privacy by Design* must be part of the overall design for smart grid data flows;
- Fortunately, in Ontario, the ‘smart metering entity’ is subject to the *Freedom of Information and Protection of Privacy Act* (FIPPA).



New Initiatives:

Collaborative Paper with NYMITY

1. Prevailing Privacy Management Myths;
 2. Understanding the Components of the Privacy Risk Optimization Process (PROP);
 3. Application of the PbD Risk Optimization Methodology;
 4. Dispelling the Myths;
- This paper introduces Nymity's *Privacy Risk Optimization Process* (PROP) into operational policies and procedures, which results in *Privacy by Design* for business practices.





Conclusions

- Lead with *Privacy by Design* – embed privacy into the design specifications of various technologies, business practices and operations;
- Take it a step further – change the paradigm from “zero-sum” to “positive-sum,” where both privacy *and* security or any functionality can be delivered, thereby raising the *overall* level of protection;
- When you change the paradigm, you change the mindset: you can deliver *both* privacy AND security, not the mutually exclusive “either/or” (false dichotomy);
- The future of privacy may very well depend on embedding privacy into design – let’s make it a reality.



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