





Privacy by Design: Going for Gold

**Michelle Chibba, Director
Information and Privacy Commissioner
Ontario**

**Information Communication Technology :
Trust in the Information Society
*León, Spain
February 11, 2010***



*We need to
change
the paradigm*



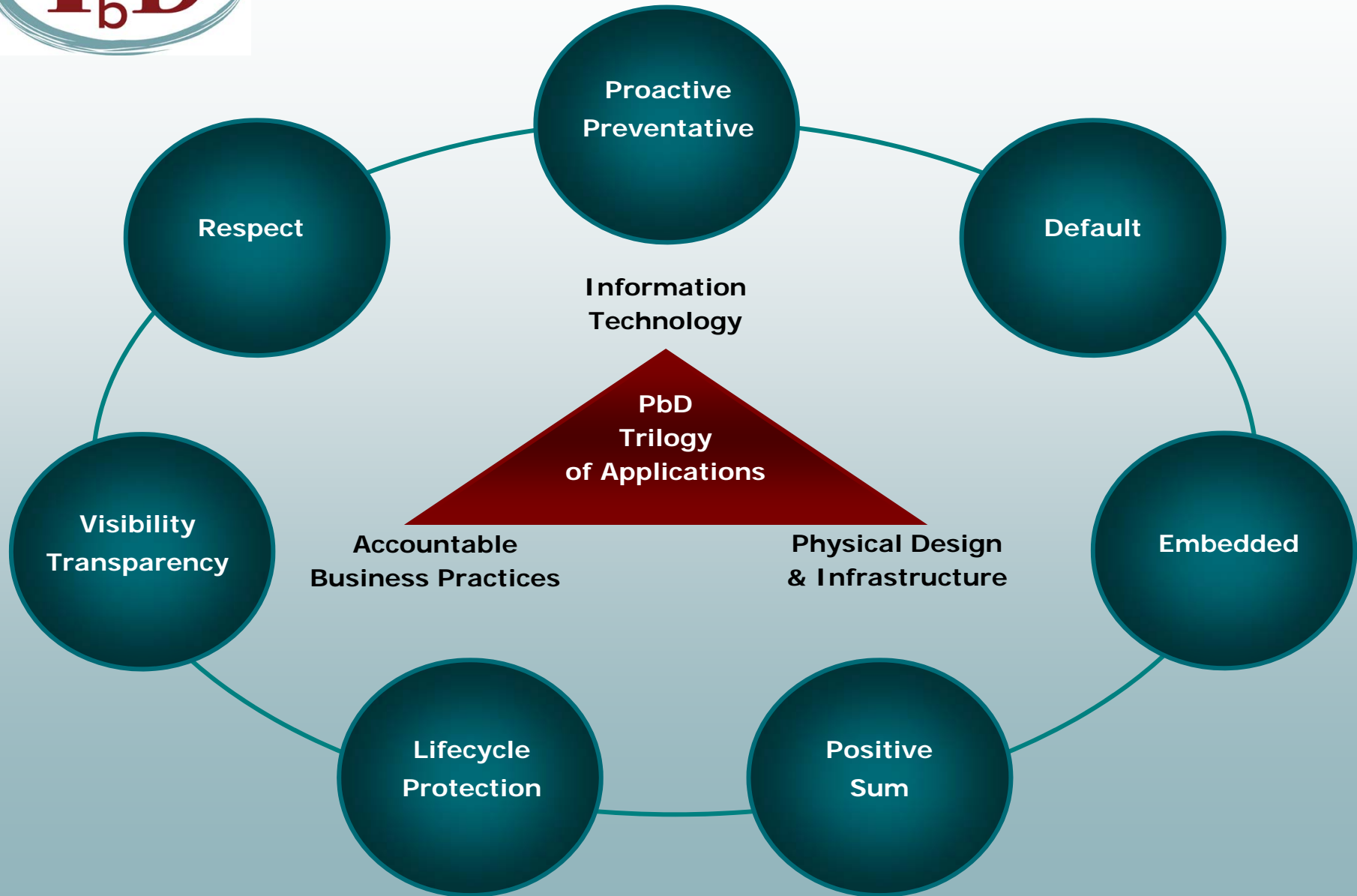
Positive-Sum Model

*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 Foundations





Privacy by Design: **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



The Next Wave:
From PETs to PETs Plus,
to
Trans Tech



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

- Examples of Transformative Techs if *PbD* enabled:
 - Biometric Encryption
 - Video Surveillance
 - RFID

**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



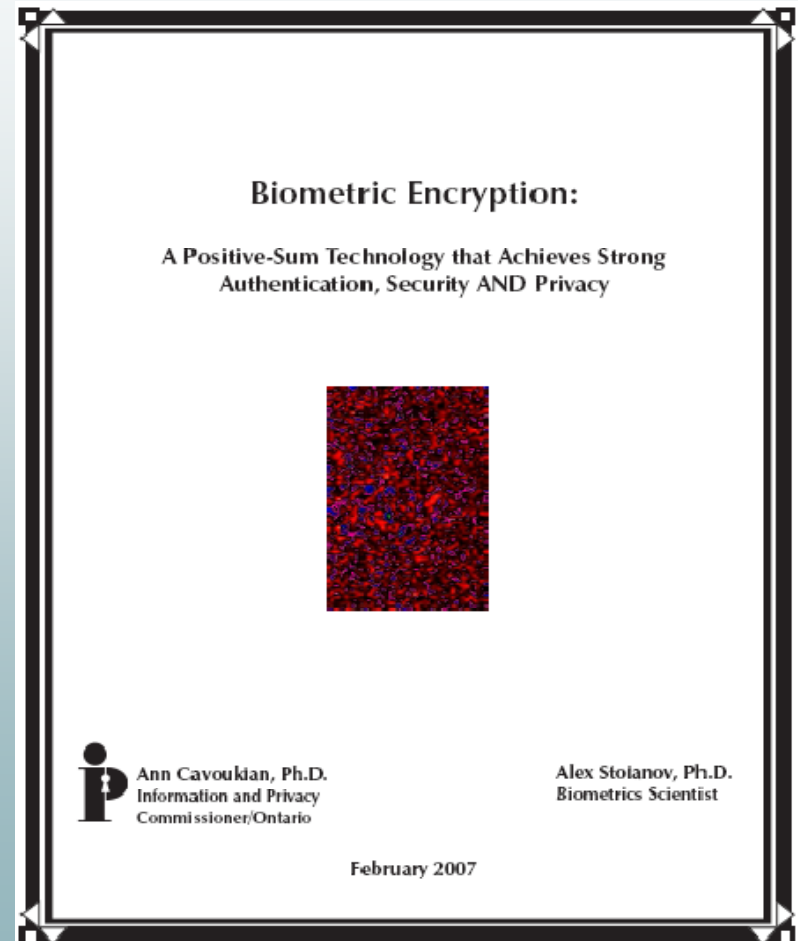
Biometrics Transformed: Biometric Encryption



Biometric Encryption:

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

- Privacy-enhanced uses of biometrics, with a particular focus on the privacy and security advantages of BE over other uses of biometrics;
- How BE technology can help to overcome the prevailing “zero-sum” mentality by effectively transforming one’s biometric to a private key.





Video Surveillance Transformed



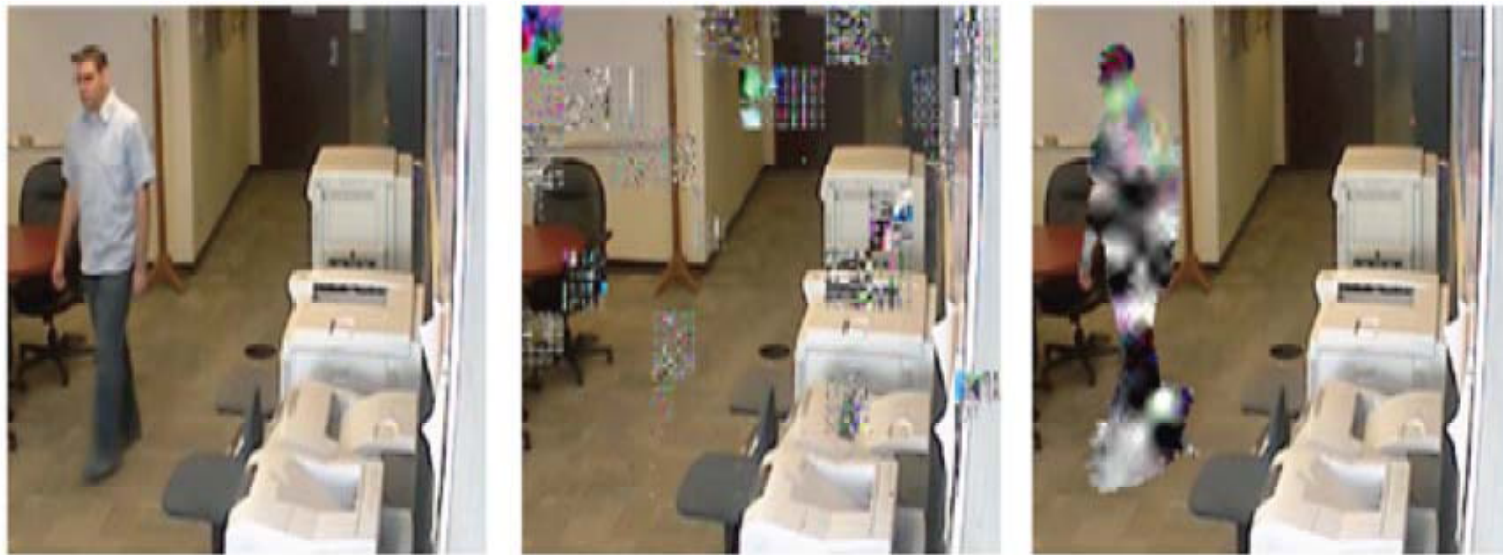
CCTV Cameras:

Innovative Privacy-Enhancing Approach to Video Surveillance

- At the University of Toronto, Professor Kostas Plataniotis and Karl Martin have developed a privacy-enhancing approach to video surveillance cameras;
- Their work, as described in *Privacy Protected Surveillance Using Secure Visual Object Coding*, uses cryptographic techniques to secure a private object (a face/image), so that it may only be viewed by designated persons;
- Objects of interest (e.g. a face or body) are stored as completely separate entities from the background surveillance frame, and strongly encrypted.



Innovative Privacy-Enhancing “Transformative” Approach



(a)

(b)

(c)

Figure (a): original content stream; Figure (b): both shape and texture have been encrypted and despite attempts to hack into this with an incorrect key, the objects of interest could not be decrypted; Figure (c): example where only the texture of the whole body (or only a face for example) is encrypted.



***RFID, Transformed:
Add an
On/Off Device***



RFID Transformed: The Solution

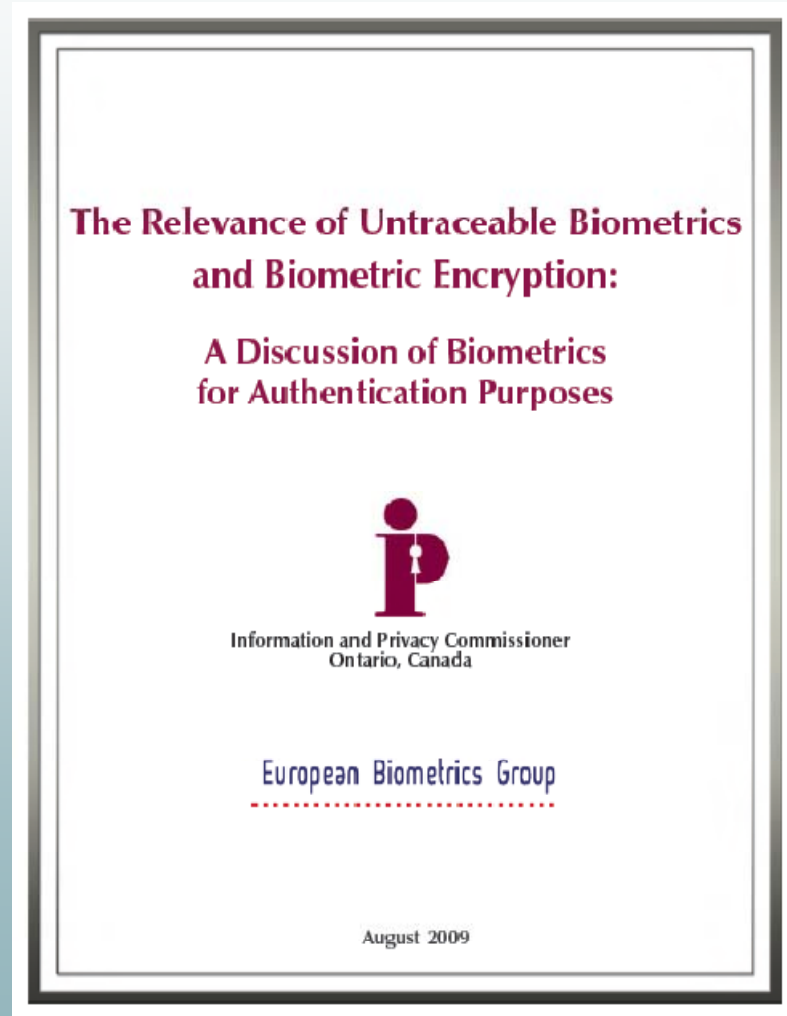
- We asked technology experts, *how can you turn it off?*
- This will have profound implications for use in RFID-enabled payment and access cards, and other forms of identification;
- Impinj® Inc., (www.impinj.com), has developed a prototype Gen2 RFID Tag (TouchTag™) that functions only when activated 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).



A Discussion of Biometrics for Authentication Purposes

- *Untraceable Biometrics*
— Ann Cavoukian, Ph.D.;
- *Anonymous Biometrics*
— Max Snijder.
- *Encyclopaedia of Biometrics:
Encryption, Biometric*
– Ann Cavoukian, Ph.D. &
Alex Stoianov, Ph.D.

www.springer.com

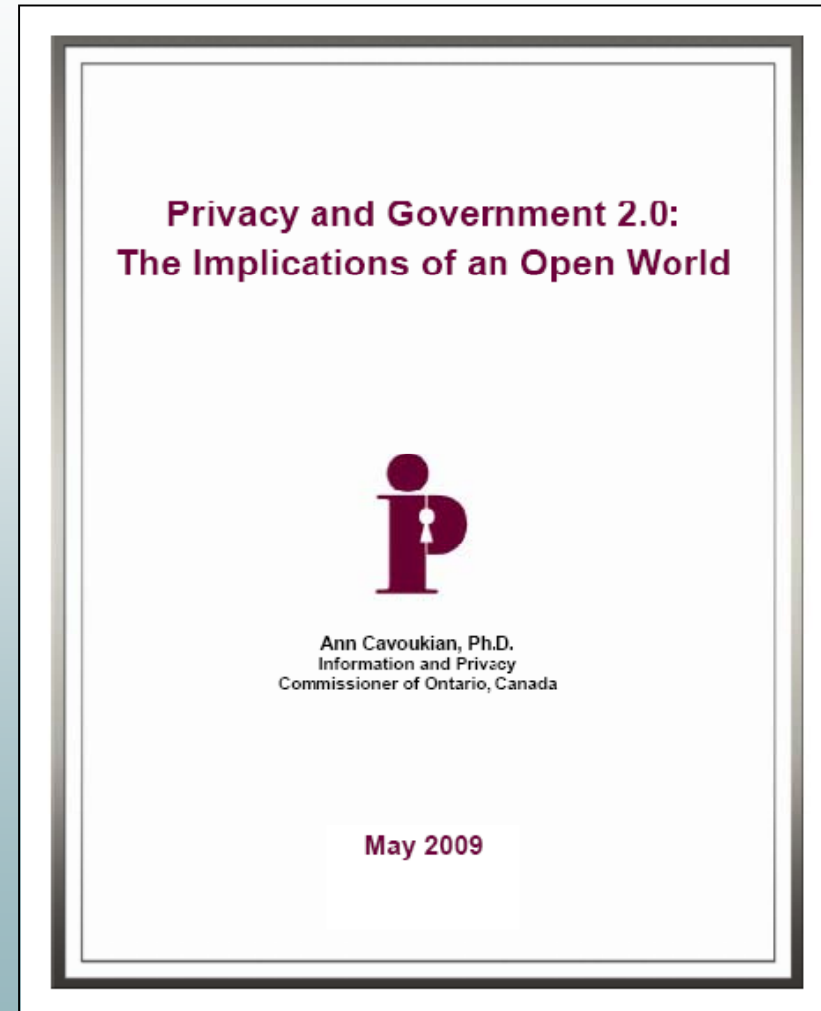


www.ipc.on.ca/images/Resources/untraceable-be.pdf



Privacy and Government 2.0

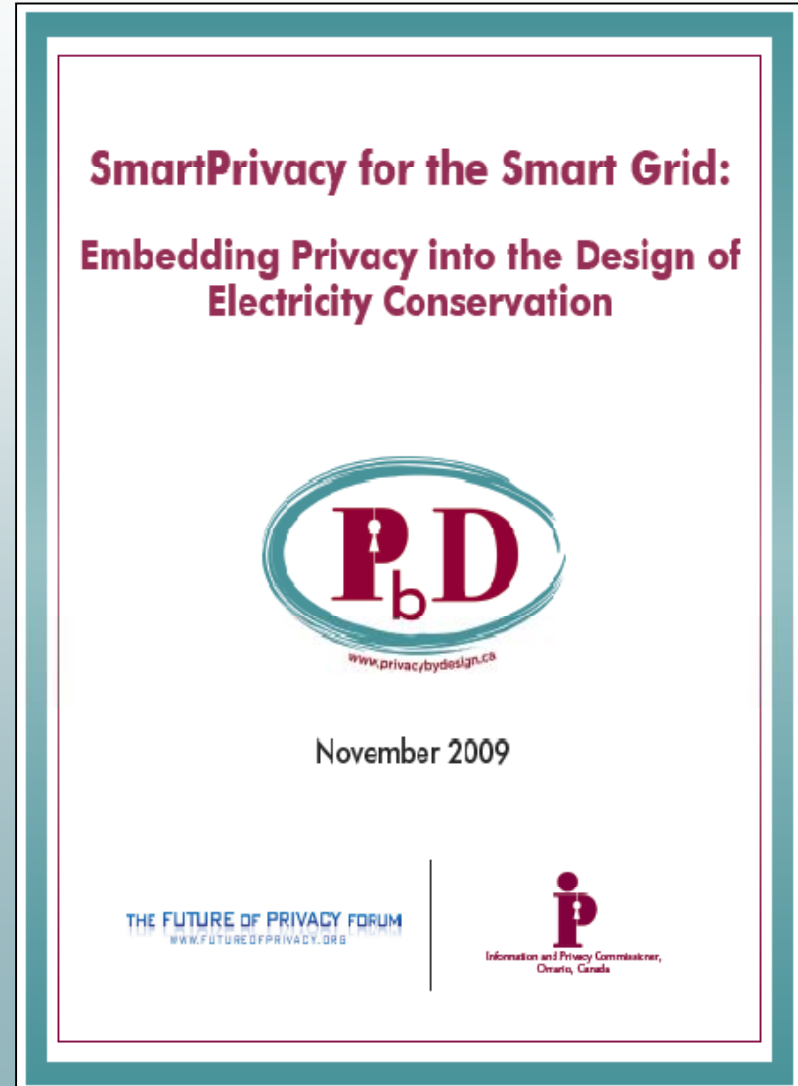
“Traditional structures of government — typically top-down hierarchical models and silo approaches — are being retired. They’re just not as compelling as they once were. With the new, function-rich infrastructure of Web 2.0, government no longer needs to work on its own to provide public value.”





SmartPrivacy for the Smart Grid

- 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);
- 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;





Why We Need *Privacy by Design*

Compliance alone, is unsustainable as a model for ensuring the future of privacy; for that, we must turn to proactive measures such as *Privacy by Design*: embedding privacy proactively into the core of all that we do.



www.smartprivacy.ca



Privacy by Design – “The sine qua non”

LAW-DEPENDENT
REGULATIONS
& RIGHTS

EDUCATION
& AWARENESS

ACCOUNTABILITY
& TRANSPARENCY

AUDIT
& CONTROL

MARKET
FORCES

Data Security

Fair Information Practices

“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, Canada, August 13, 2009.



A Research Program

Privacy and security in a virtual web-world

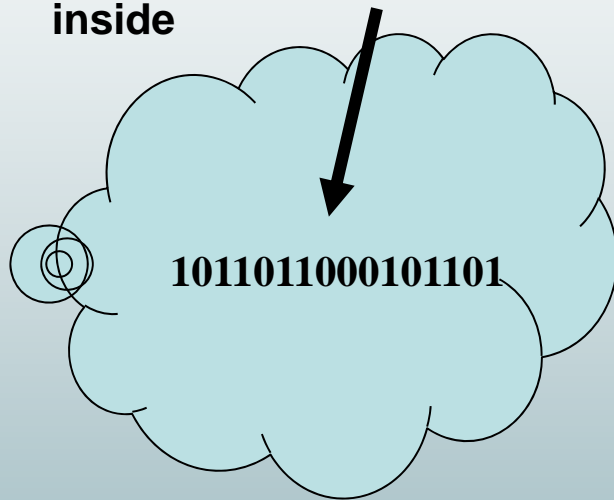
SmartData:
Make the data “think” for itself

George J. Tomko, Ph.D.
Expert-In-Residence
Identity, Privacy and Security Institute (IPSI)
University of Toronto, Canada



No Personal information in the Cloud: Just SmartData

SmartData binary string –
personal information locked
inside



- There would be no personal or proprietary “raw” data out in the open.
- It would instead be housed “within” a SmartData agent



*SmartPrivacy
is Smart Business*



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*



Costs of a Privacy Breach

- Legal liabilities, class action suits;
- Loss of client confidentiality and trust;
- Diminution of brand and reputation;
- Loss of customers, competitive edge;
- Penalties and fines levied;
- Costs of crisis management, damage control, review and retrofit of information systems, policies and procedures.



Good Governance and Privacy: *Board of Directors*

IPC Publication:

- Guidance to corporate directors faced with increasing responsibilities and expectation of openness and transparency;
- Privacy among the key issues that Boards of Directors must address;
- Potential risks if Directors ignore privacy;
- Great benefits to be reaped if privacy included in a company's business plan.





Bottom Line: *It's All About Trust*

“...trust remains essentially the ‘classical’ concept we know, and which needs transposition to the new digital space.”

— RISEPTIS

Trust in the Information Society



Conclusions

- Lead with *Privacy by Design* – embed privacy into the design specifications of information technologies, accountable business practices and operations;
- Take it a step further – change the paradigm from “zero-sum” to “**positive-sum**,” where both privacy *and* security can be delivered, thereby raising the *overall* level of protection;
- *Privacy by Design* was not developed for use in an ivory tower. It was developed to introduce real changes to our everyday lives with regards to protecting our privacy – we invite everyone to participate in that process.



How to Contact Us

Michelle Chibba, Director

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