

Privacy by Design:
A Call to Action

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner
Ontario

Center for Advancing Business through Information Technology
Arizona State University – W.P. Carey School of Business
November 24, 2009



Presentation Outline

- 1. We Need to Change the Paradigm*
- 2. SmartPrivacy and Privacy by Design*
- 3. The Next Wave: From PETs to PETs Plus,
... to Transformative Technologies*
- 4. Biometrics Transformed: Biometric Encryption*
- 5. Video Surveillance Transformed*
- 6. RFID Transformed: Add an On/Off Switch*
- 7. SmartPrivacy for the Smart Grid*
- 8. SmartPrivacy is Smart Business*
- 9. Conclusions*



*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*



Why We Need Technology to Protect Privacy

“We need technology ... citizens need technology to protect themselves because the law is *not* doing it.”

— Jennifer Granick

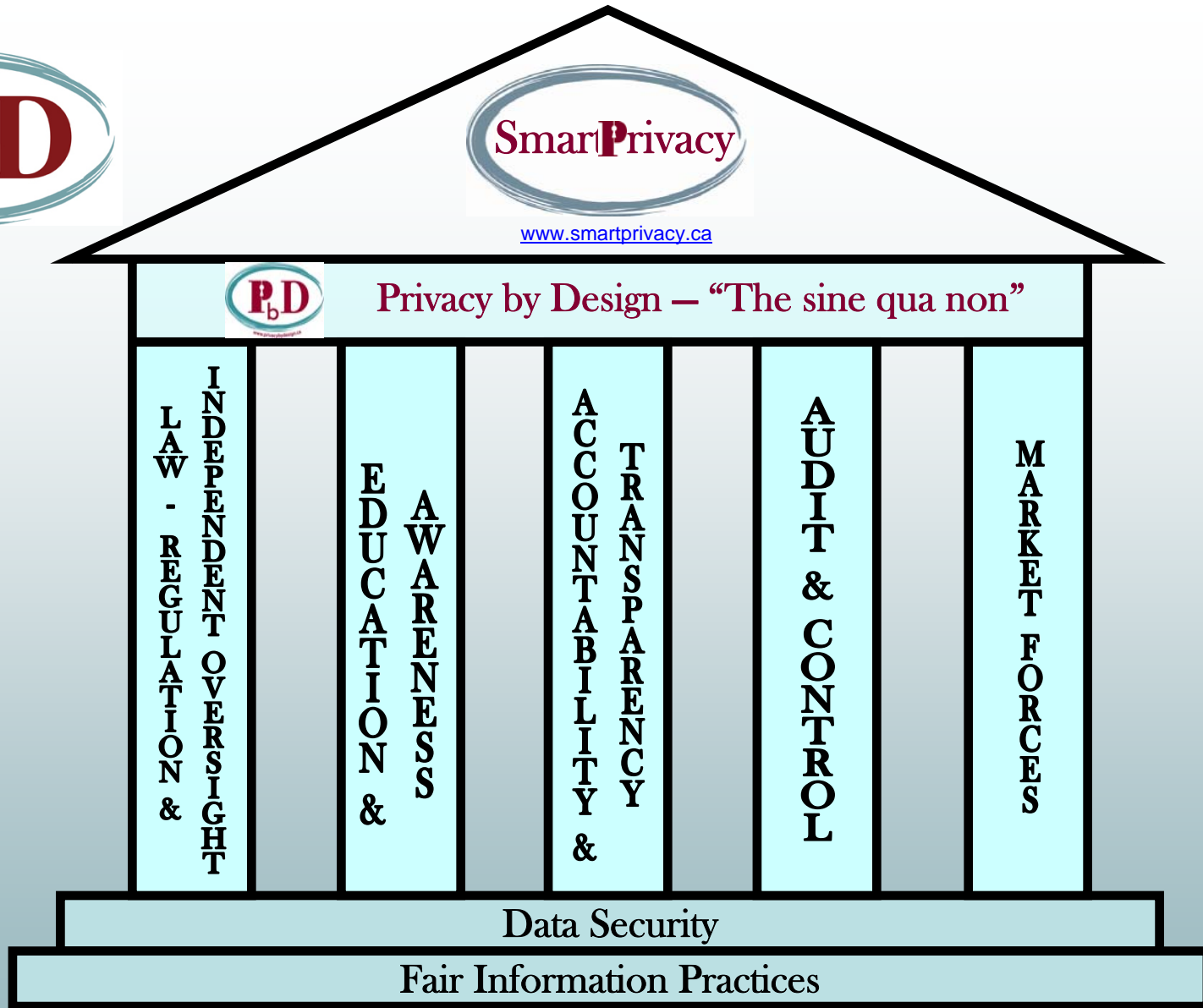
Electronic Frontier Foundation



*SmartPrivacy
and
Privacy by Design*



www.smartprivacy.ca



"SmartPrivacy is the umbrella that offers the complete suite of protections to ensure data privacy. It consists of multiple measures ranging from regulatory protection to Smart Privacy Foundations, 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.



www.privacybydesign.ca



ASU *PbD* Research Lab

**The world's first
Privacy by Design Research Lab
will be at Arizona State University**



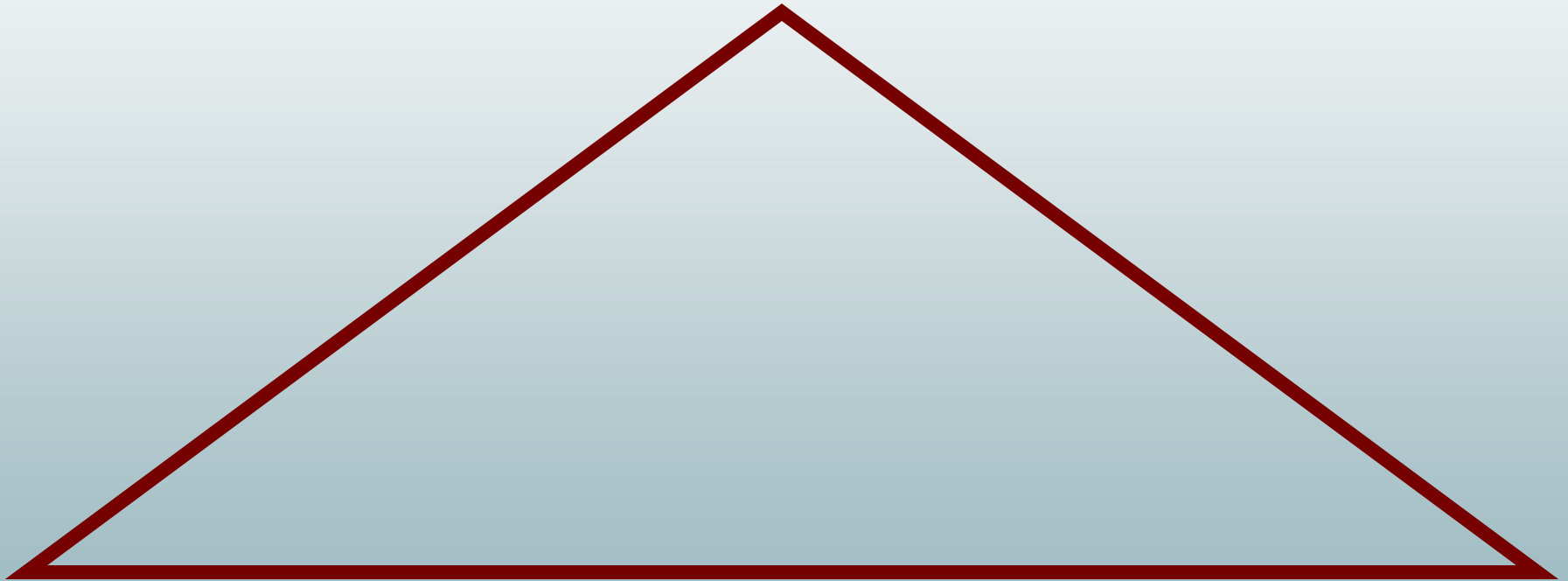
Privacy by Design: “Build It In”

- 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.



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.



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 proactive measures such as *Privacy by Design*: embedding privacy proactively into the core of all that we do.




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



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.



Become a *Privacy by Design Ambassador*

Become a Privacy by Design Ambassador:

1. Identify within your organization an emerging technology, business practice or infrastructure that intersects with personally identifiable information and work toward building the principles of Privacy by Design (PbD) into it.
2. Share your ideas in our “PbD Community Forum.” Go to www.privacybydesign.ca. Participate in the community, to provide your insights, and assist others in implementing the PbD principles.
3. Spread the message! Whenever you find the opportunity, inform others about the advantages and benefits of Privacy by Design.

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 – I invite everyone to participate in that process.



The Next Wave:

From PETs to PETs Plus,

to

Trans Tech



Background:

Privacy-Enhancing Technologies (*PETs*)

- The IPC and the Dutch Data Protection Authority advanced 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 (not-zero-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
 - 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



IPC and Biometrics

- The IPC has been a longstanding proponent of biometric encryption technologies;
- We continue to press for strong privacy protections in the development and deployment of interoperable biometric technologies;
- Active member of the European Biometrics Forum International Biometrics Advisory Council (IBAC).

www.eubiometricforum.com/index.php?option=content&task=view&id=457



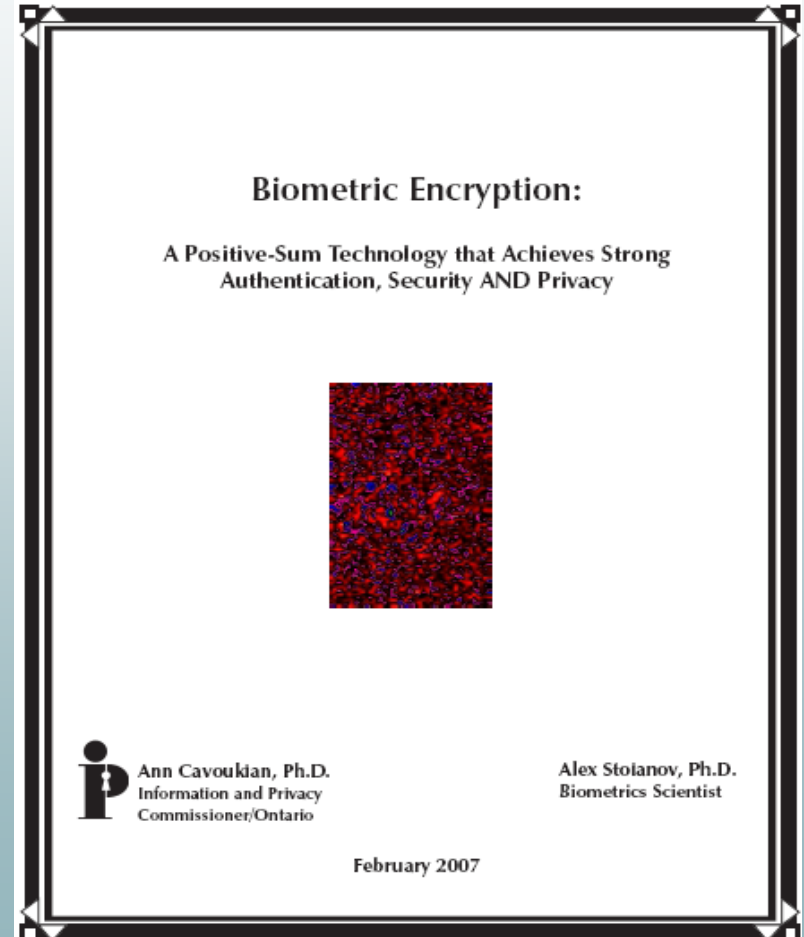
European Biometrics Forum

- The European Biometrics Forum (EBF) was launched in 2003; Member of International Biometrics Advisory Council (IBAC);
- Composed of leading biometrics and technology experts, the EBF was established to develop world-class standards, best practices and innovation in the biometrics industry to strengthen trust and confidence in the use of emerging biometric applications;
- The EBF is supported by a network of national biometric organizations, companies, universities and experts across Europe in carrying out research for the development of a roadmap for the European Biometrics industry to 2010.



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.





Biometric Encryption (BE)*

What is Biometric Encryption?

- Class of emerging “untraceable biometric” technologies that seek to transform the biometric data provided by the user;
- Special properties:
 - uniqueness
 - irreversibility

* Pioneering development by George Tomko, Ph.D.
Founder of Mytec Technologies, 1994.



Biometric Encryption

- Biometric encryption is a process that securely binds a PIN or a cryptographic key with a biometric, so that neither the key nor the biometric can be retrieved. The key is recreated only if the correct live biometric sample (a finger or iris) is presented on verification;
- In biometric encryption, you can use the biometric to encrypt a PIN or a password for numerous applications, such as access to computers or bank machines. The PIN can be 100s of digits in length since you don't need to remember it;
- Most important, the only item that has to be stored in a database is the biometrically encrypted PIN or password, not the biometric template, so privacy is preserved.



Current BE Projects

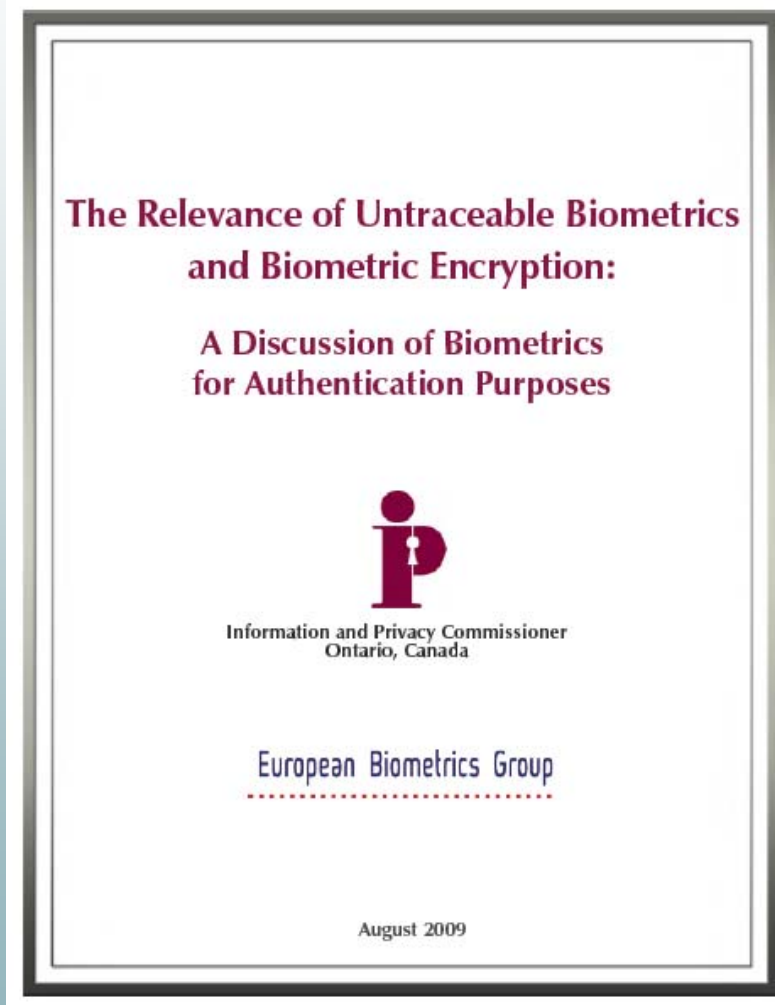
- **The Philips privID™ (Netherlands)** – is currently one of the most advanced BE technologies in operation; unlike some BE systems, the privID™ system is very fast which allows for a true one-to-many mode; it is also very secure, making it extremely difficult to crack;
- **PerSay (Israel)** – has successfully combined their own voice authentication technology with Philips' BE technology making voice biometric encryption a reality;
- **Ontario Lottery and Gaming (OLG)** – Professor Kostas Plataniotis and Karl Martin, University of Toronto, have developed a privacy-enhancing approach to video surveillance cameras using cryptographic techniques so that it may only be viewed by unlocking the encrypted object with a secret key. The OLG is now exploring the possibility of using this technology for their self-exclusion program.



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



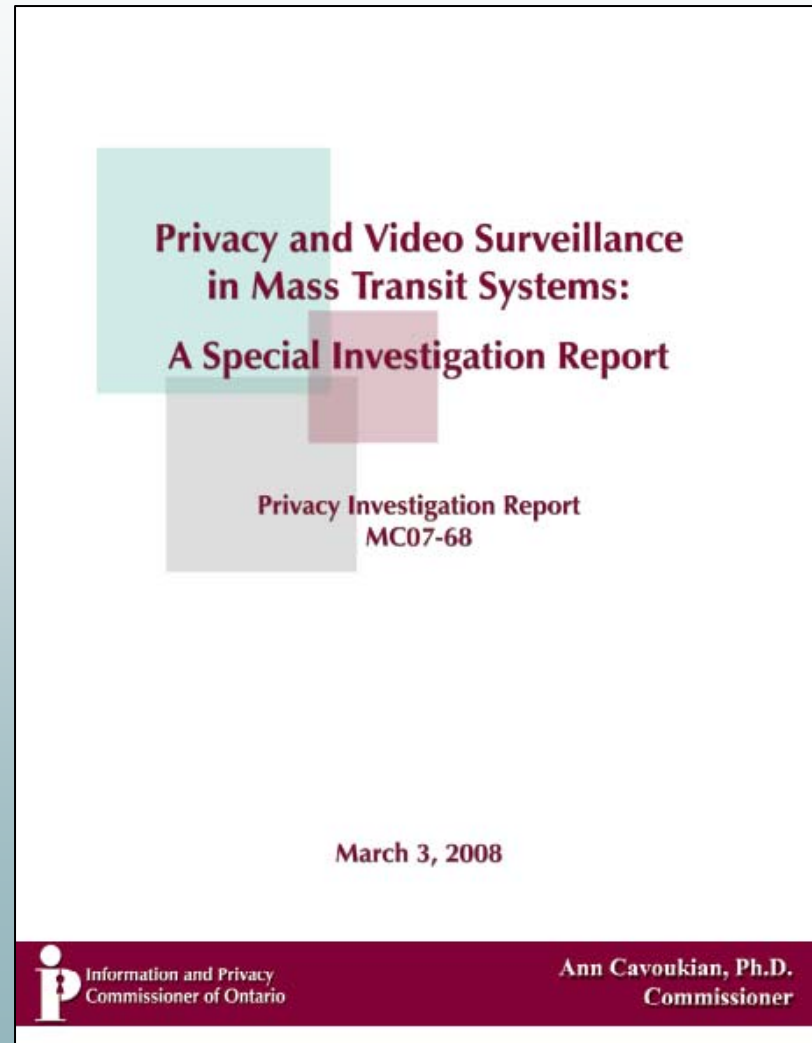


Video Surveillance Transformed



TTC Surveillance Cameras

- In March 2008, I ruled that Toronto's Mass Transit System's use of video surveillance cameras was in compliance with Ontario's privacy law.
- However, I called upon the TTC to undertake a number of specific measures to enhance privacy:
 - Personal information will only be collected for legitimate, limited and specific purposes;
 - Collection will be limited to the minimum necessary and **only retained up to 72 hours;**
 - A comprehensive audit of the video surveillance system must be conducted by an independent third party using the GAPP (Generally Accepted Privacy Principles).





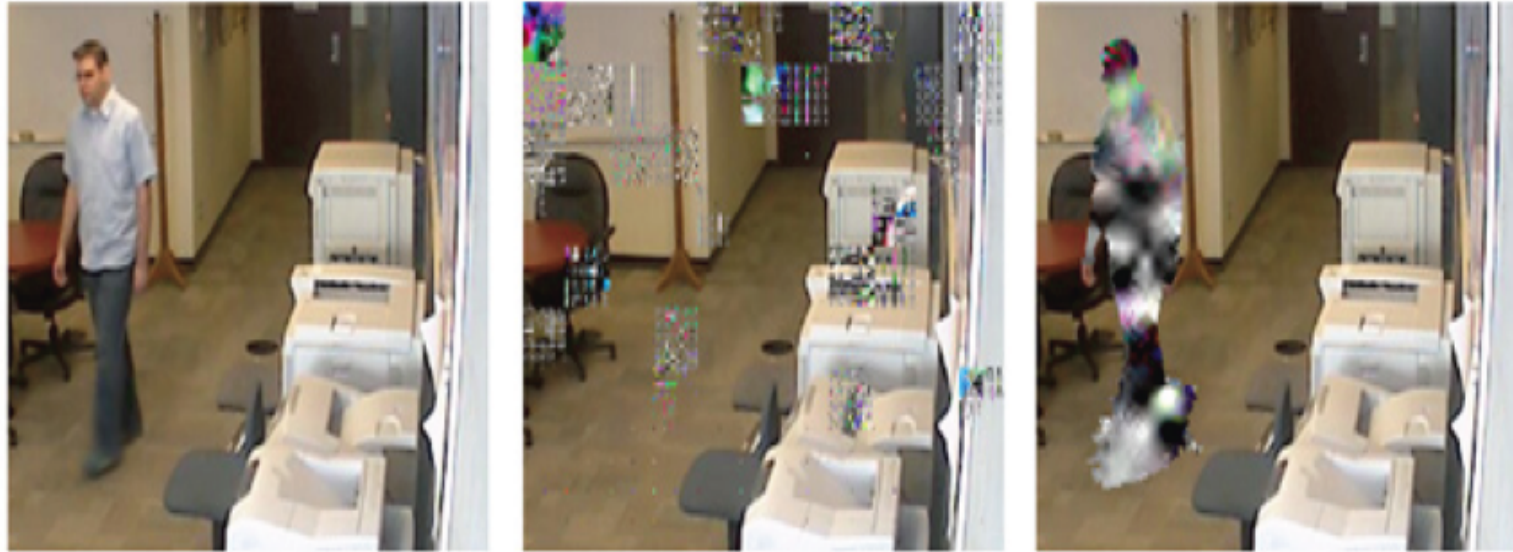
CCTV Cameras:

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.



TTC Report: What the Experts are Saying

“The report is a valuable step forward toward ensuring that video surveillance be carried out in ways that ensure that privacy is protected and that oversight exists.”

— Professor Daniel J. Solove, Associate Professor of Law,
George Washington University Law School

“While I understand your report is specifically addressing only the Toronto Transit Commission, it will be invaluable to municipalities throughout the world which are facing similar vexing questions about the proper use and management of video surveillance technologies. Your recommendations provide a principled yet workable model for how to protect individuals' legal and moral right to privacy while also advancing the public's interest in safe, efficient and affordable infrastructure.”

— Professor Fred Cate, Distinguished Professor of Law and
Director, Center for Applied Cybersecurity Research



TTC Report: What the Experts are Saying (Cont'd)

“It sets the bench mark for informed discussion of CCTV in mass transit systems ... It provides a roadmap for the most privacy protective approach to CCTV. It offers potential technological solutions that can further enhance privacy with CCTV imagery. It presents specific recommendations and a requirement for an independent third-party audit (this is the Commissioner flexing her muscles). Finally, it demonstrates that ... good system design, vigilant oversight, and a commitment to privacy values can result in ‘positive-sum’ models as Commissioner Cavoukian describes them.”

— Murray Long, Editor and Publisher,
PrivacyScan



Toronto Police Services

Surveillance Cameras

- The Toronto Police Service (TPS) conducted a pilot project to test Closed Circuit Television (CCTV) video surveillance in specific high-crime areas, as an added tool for the detection and deterrence of crime and enhancing public safety and security;
- Members of the TPS met with the IPC to apprise us of this proposal. The Police were aware of the IPC's *Guidelines for Using Video Surveillance Cameras in Public Places* and stated their intention to adhere to them;
- IPC personnel conducted a site visit at the outset of the pilot project, and the TPS kept the IPC informed of developments during the program, which concluded with an evaluation in Spring 2008.



Toronto Police Services

Support for Positive-Sum Approach

“This governance model has ensured a **positive-sum approach** to the use of public space cameras in Toronto, one that enables the use of this additional tool to support policing while concurrently mitigating privacy concerns through technological and operational design.”

— Chief of Toronto Police Services, William Blair,
October 22, 2009.



***RFID, Transformed:
Add an
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?*
- 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).



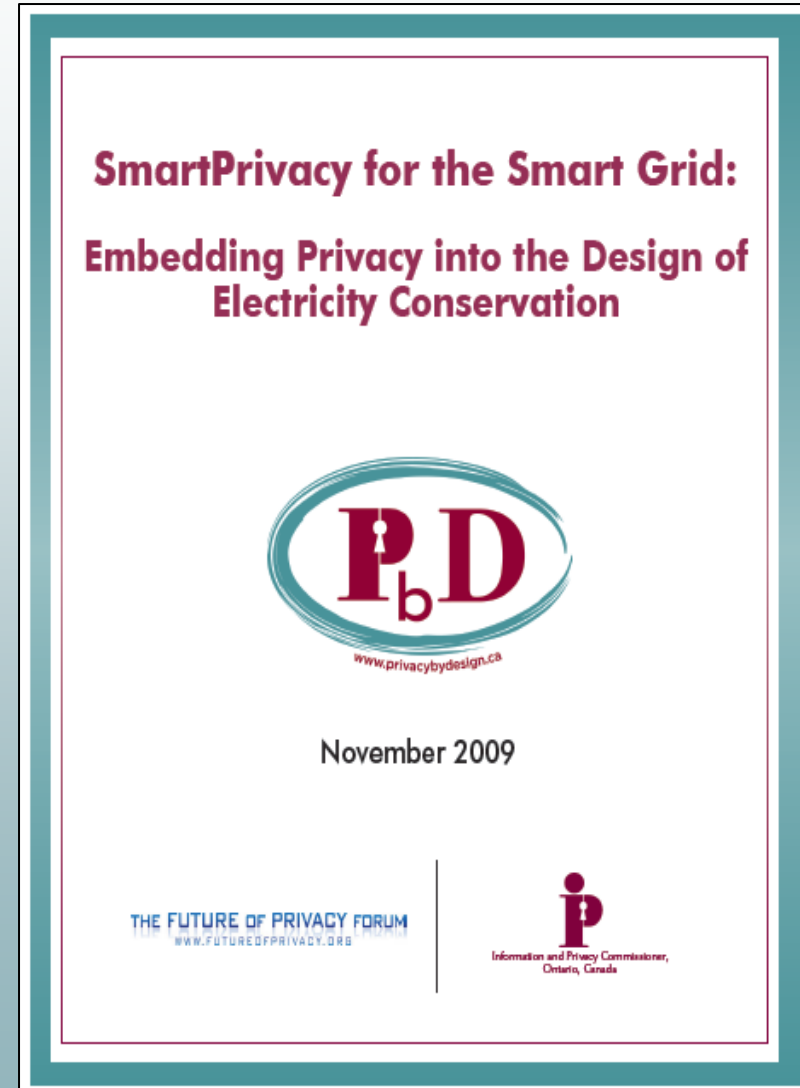
*SmartPrivacy for the
Smart Grid*



SmartPrivacy for the Smart Grid

- Released November 2009, with the Future of Privacy Forum.

www.privacybydesign.ca





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).



*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*



Consumer Choice and Privacy

- There is a strong competitive advantage for businesses to invest in good data privacy and security practices;
- *“There is a significant portion of the population that is becoming concerned about identity theft, and it is influencing their purchasing decisions.”*

— Rena Mears, Deloitte & Touche LLP



Costs of a Privacy Breach

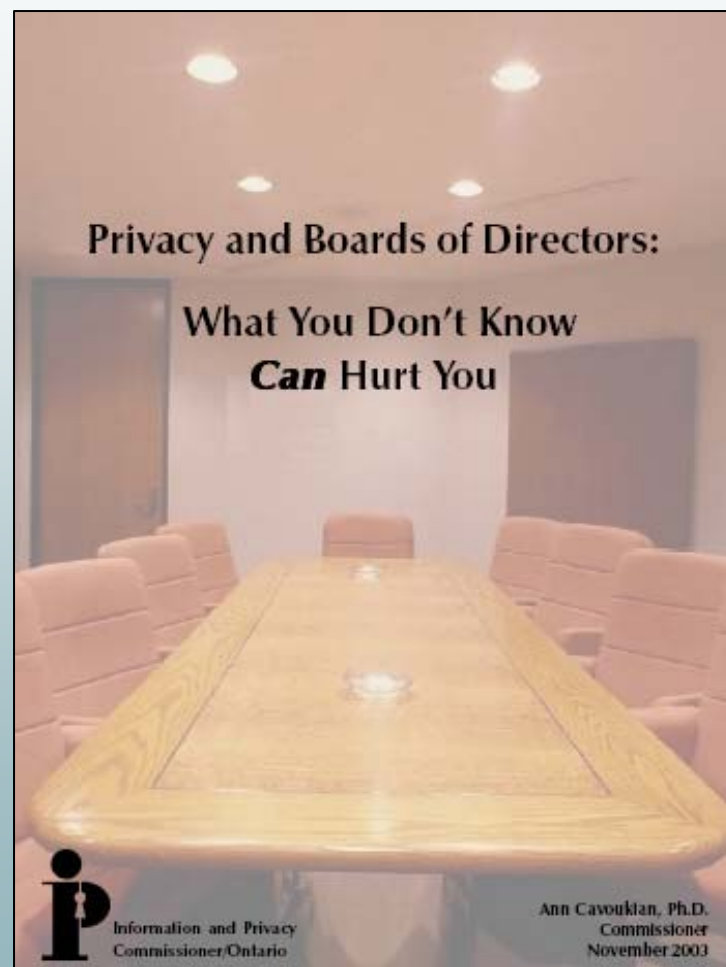
- Legal liabilities, class action suits;
- Loss of client confidentiality and trust;
- Diminution of brand and reputation;
- Loss of customers, competitive edge;
- Penalties and fines levied;
- Costs of crisis management, damage control, review and retrofit of information systems, policies and procedures.



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 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*



Ten Reasons for Building Consumer Trust

1. Avoiding damage to your company's and/or brand's reputation;
2. Avoiding penalization by any existing or pending laws;
3. Avoiding civil and class-action lawsuits;
4. Maintaining the balance of monitoring the activities of employees while not harming their morale and productivity;
5. Ensuring the continuation of valuable business relationships by ensuring your company measures up to the privacy standards adopted by strategic partners;



Ten Reasons for Building Consumer Trust (Cont'd)

6. Being aware of the privacy laws and customs in other countries;
7. Gaining the trust and confidence of customers so that they will not provide you with false information;
8. Dealing with consumers who expect you to treat their personal information the same way that you would treat your own;
9. Repeat online customers are those that feel assured that shopping online is secure and that their information is protected;
10. Gain and maintain an edge over your competitors through embracing more than just the minimum of laws, regulations and privacy best practices.

— Ann Cavoukian, Ph.D., Tyler Hamilton, *The Privacy Payoff: How Successful Business Build Consumer Trust*, McGraw-Hill Ryerson, 2002, pp. 13-14.



Managing Organizational Data

- Does your organization have a Data Map?
- Do you know all the points of entry for personally identifiable information (PII) into your organization?
- Do you know how customer data flows throughout your organization?
- Do you have a consent management system in place ... when you need to obtain additional consent from your customers?



Federated Privacy Impact Assessment (F-PIA)

Goals of an F-PIA:

- Provide an opportunity for members to develop and codify a Federation's privacy policies;
- Demonstrate that privacy policies, as defined by members of the Federation, will be met;
- Demonstrate that an appropriate technological architecture is in place to prevent, to the extent possible, accidental or malicious violations of privacy policies.





– 2010 –

Stay tuned for another new tool: Moving from PIA to “PRA”

- The idea for a **Privacy Risk Assessment (PRA)** assessment tool was first envisioned at the annual Risk and Insurance Management Society (RIMS) conference in late 2008;
- My office formed a collaborative working group with Sun Life Financial and the YMCA to develop a new tool to build a bridge between risk management and privacy concerns;
- Stay tuned – it’s coming to Boston in April, 2010.



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;
- When you change the paradigm, you then change the mindset: you can deliver *both* privacy AND security, not as mutually exclusive “either/or” (false dichotomy) but also doubly enabling “win/win;”
- 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