Change the Paradigm, Change the Practice: Lead with "Privacy by Design"

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

10th Annual Reboot Privacy and Security Conference
Victoria, British Columbia
February 3, 2009

Presentation Outline

1. *The Privacy Landscape*
2. *The Future of Privacy: Positive-Sum, NOT Zero-Sum*
3. *The Next Wave: From PETs to PETs Plus, … to Transformative Technologies*
4. *Biometrics, Transformed: Biometric Encryption*
5. *Video Surveillance, Transformed: Secure Visual Object Coding*
6. *RFID, Transformed: QTC On/Off Device*
7. *We're Changing the Paradigm*

The Privacy Landscape

Privacy = Freedom

What Privacy is Not

Privacy ≠ Security

Security *is*, however, vital to privacy

What is Needed:

Privacy

and

Security,

not

one or the other

Information Privacy Defined

Information Privacy: Data Protection

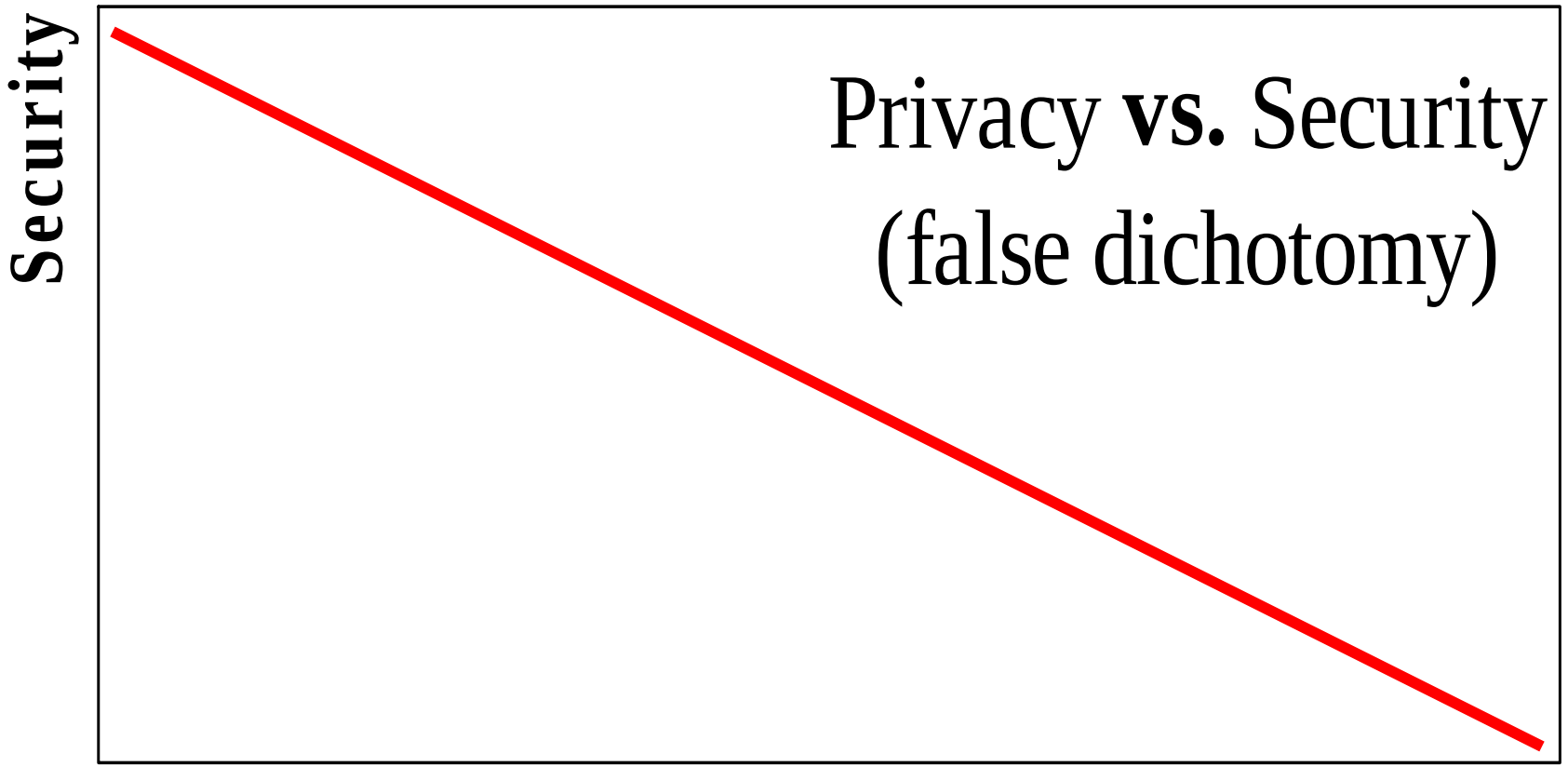
- Freedom of choice; personal control; informational self-determination;
- Control over the collection, use and disclosure of any recorded information about an identifiable individual;
- Privacy principles embodied in "Fair Information Practices;"
- Global Privacy Standard (2006). www.ipc.on.ca/images/Resources/up-gps.pdf

If Privacy is to Survive, Things Have to Change

The Future of Privacy:

Positive-Sum
NOT
Zero-Sum

Privacy OR Security:
A Zero-Sum Game



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 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, delivering a "win-win" outcome.

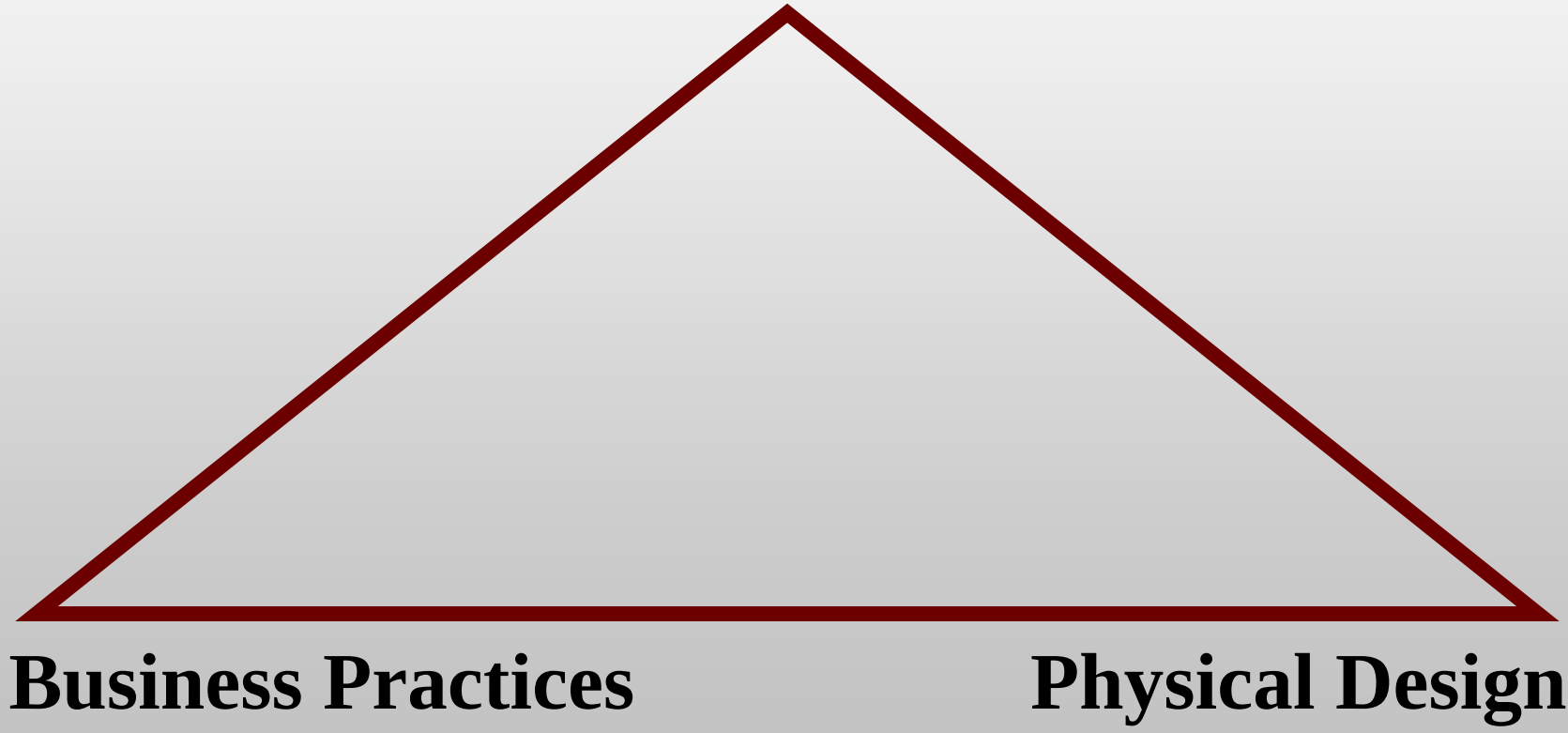
Positive-Sum Model

Change the paradigm
from "zero-sum" to
a "positive-sum" model:
Create a "win-win" scenario,
not an "either/or"
involving unnecessary
trade-offs

Privacy by Design: "Build It In"

- I first developed the term "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 Trinity of Applications



The Next Wave:

From PETs to PETs Plus, to Trans Tech

Background: Privacy-Enhancing Technologies *(PETs)*

- The IPC 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 the landmark study, *Privacy-Enhancing Technologies: The Path to Anonymity (Vols. I & II).*

  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

Surveillance Technology + Positive-Sum Paradigm + Privacy-Enhancing Technology =

<u>Transformative Technology</u>

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.

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

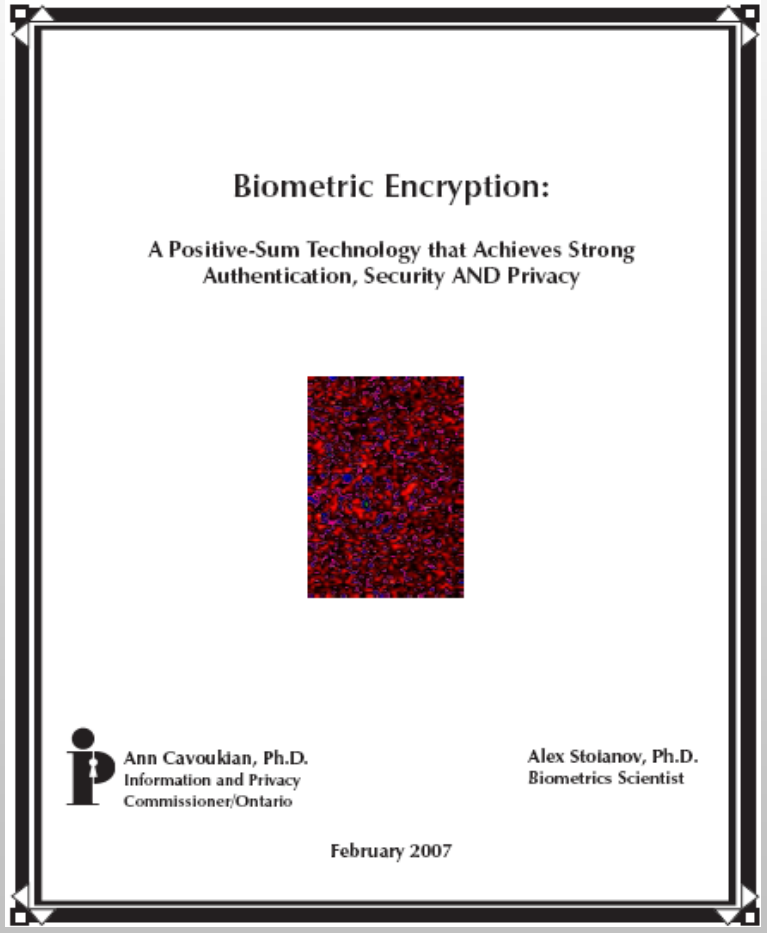
- The European Biometrics Forum (EBF) was launched in 2003; Member of International Biometrics Advisory Council (IBAC);
- Composed of leading biometrics and technology experts, the EBF was established to develop world-class standards, best practices and innovation in the biometrics industry to strengthen 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.

www.eubiometricforum.com

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.



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

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.

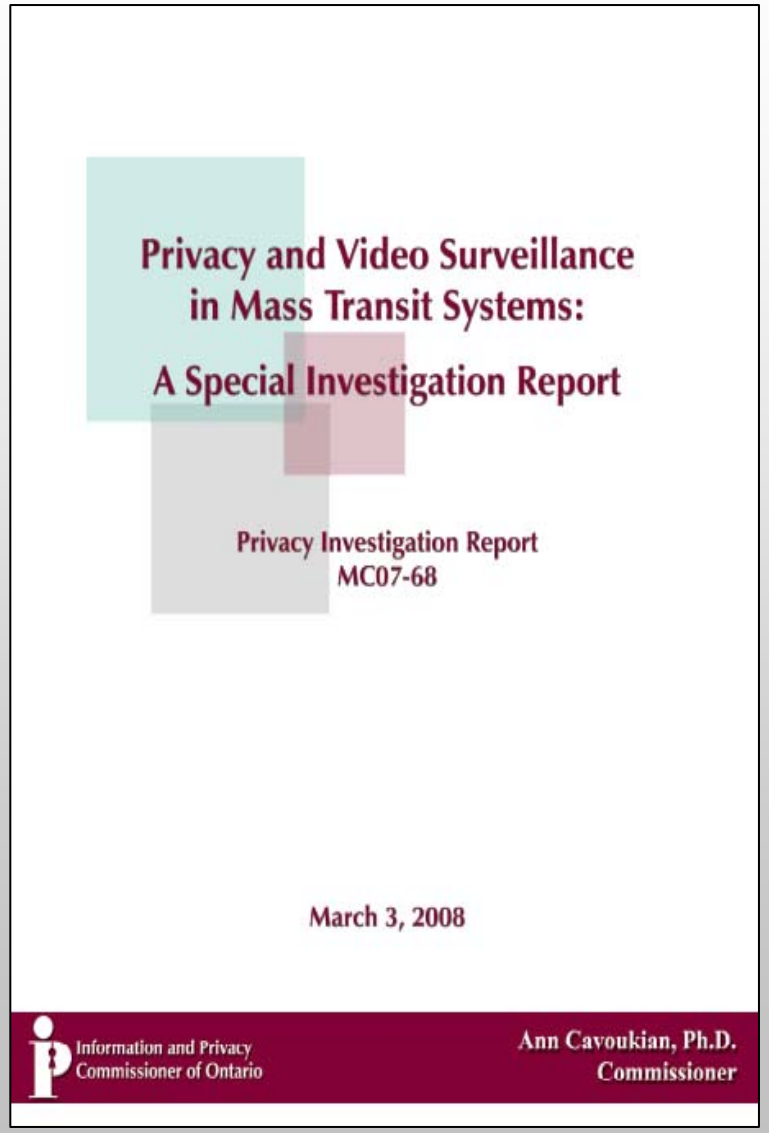
Current BE Projects

- **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. A major telecommunications company is now exploring the possibility of deploying a voluntary voice identity verification service for its customers using this new technology;

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).

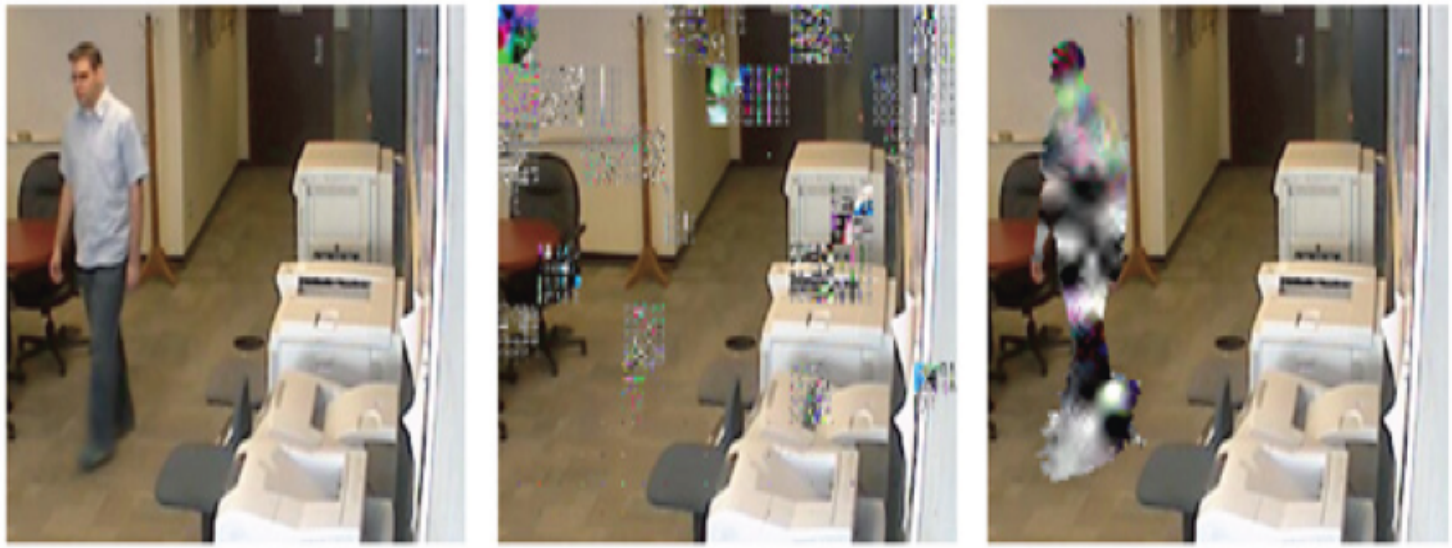


www.ipc.on.ca/images/Findings/mc07-68-ttc.pdf

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 (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

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

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*, unless the user chooses to turn it *on*, when needed.

RFID Transformed: The Solution

- We asked those in the know, *how can you turn it off?*
- Peratech, (www. peratech.com), a UK-based developer of an innovative new super-slim conductive material called *QTC*, has developed a working prototype on/off switch that can be embedded into any ID card, with a high degree of reliability and durability;
- When pressed by the user, this switch connects the RFID chip to the antenna, allowing the RFID chip to be remotely read; the user is in control – the RFID is engaged when needed;
- This is an exciting transformative technology that addresses fundamental security and privacy concerns *without* interfering with current border program plans – positive-sum;
- Profound implications for use in RFID-enabled payment and access cards, and other forms of identification.

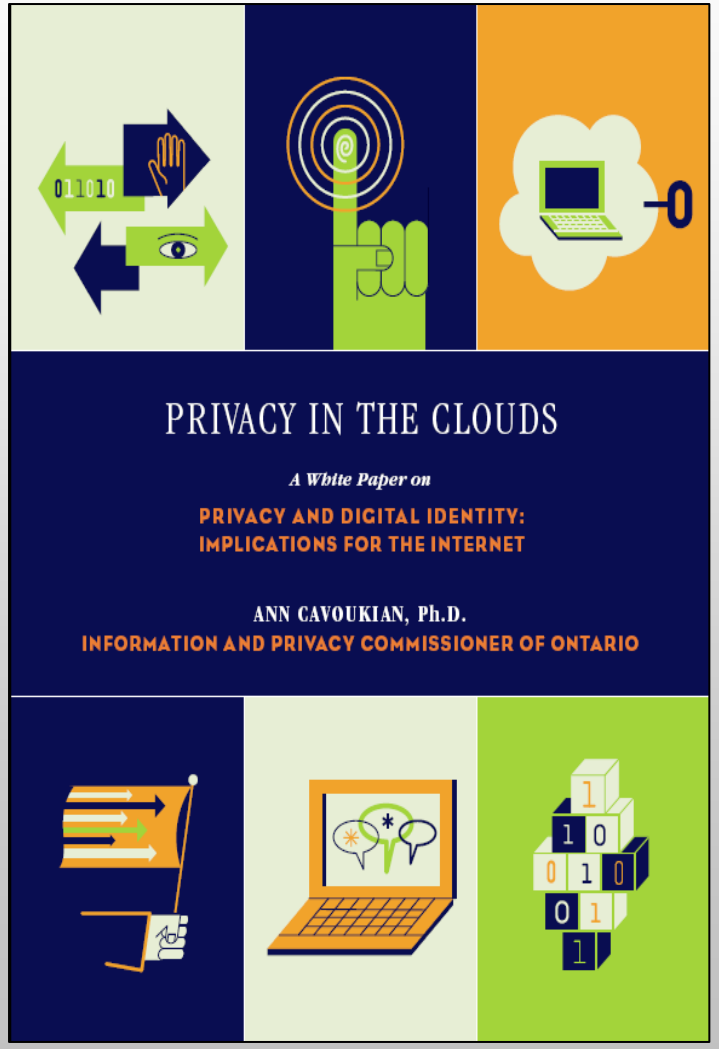
We're Changing the Paradigm

New IPC Initiatives

Privacy in the Clouds
(in the Web 2.0 World)

Cloud Building Blocks:

1. Open source and proprietary identity software based on open standards;
2. **FEDERATED IDENTITY**;
3. Multiple and partial identities;
4. Data-centred policies;
5. Audit tool.



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

Announcing a New PIA: The *"F-PIA"*

- Today we're announcing the launch of a new PIA for use in a Web 2.0 world:

Federated Privacy Impact Assessment
"(F-PIA)"

- To be released in approximately one hour at 11:00, at Panel A on Cloud Computing (in the Theatre).

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 "PRM"

- The idea for a **Privacy Risk Management (PRM)** 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 in the Spring of 2010.

Conclusions

- Let's lead with Privacy by Design – embedding privacy into the design specifications of various technologies and business practices;
- Take it a step further – change the paradigm from "zero-sum" to "positive-sum," where both privacy *and* security can be delivered, raising the *overall* level of protection provided;
- When you change the paradigm, you change how you think: you can deliver *both* privacy AND security, not the mutually exclusive "either/or;"
- 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