Privacy Through Technology: Lead by Using a Positive-Sum Paradigm

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario

Insurance-Canada Technology Conference
Leadership: The Business-IT Imperative
February 23, 2009

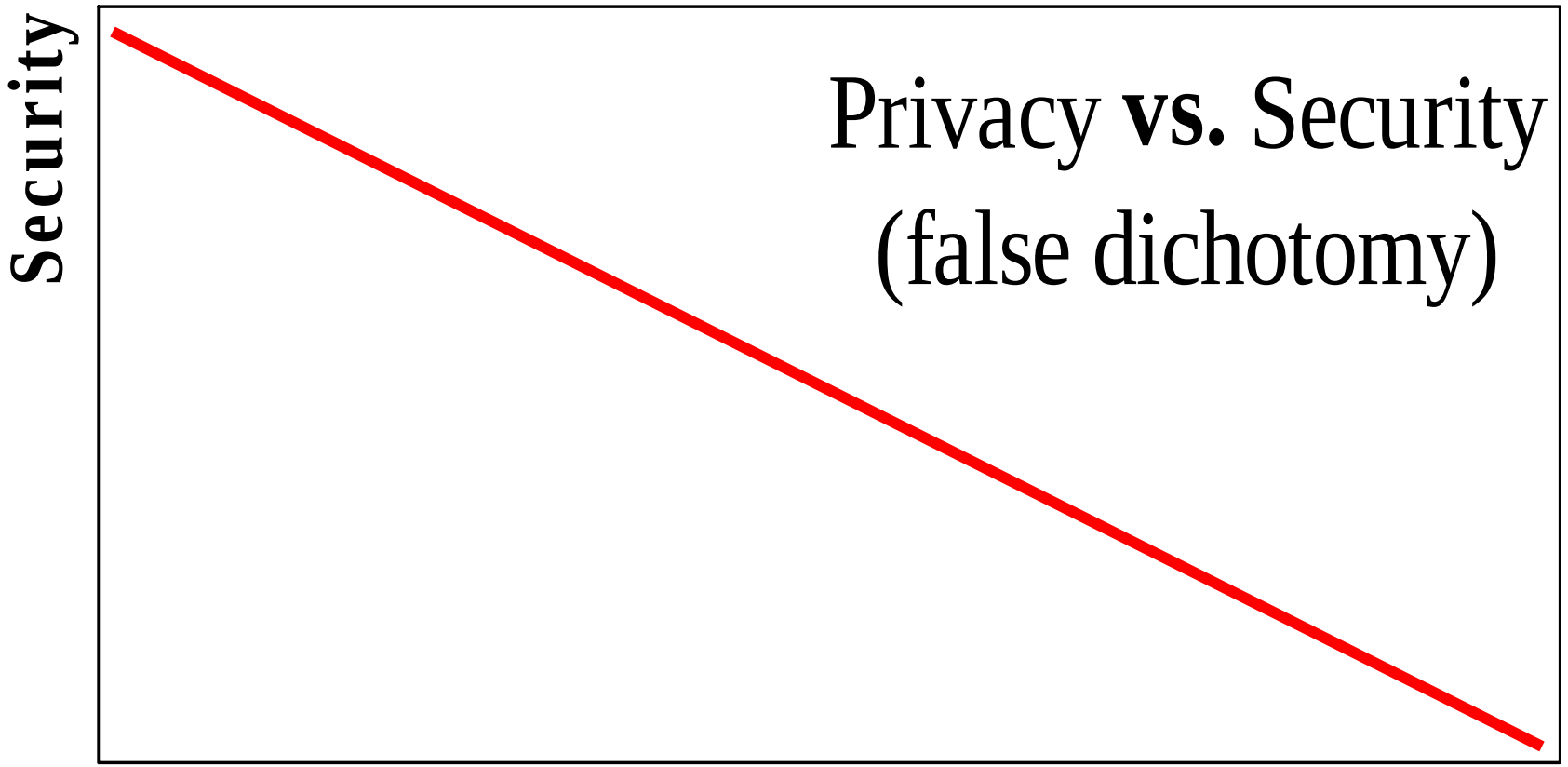
Presentation Outline

1. *The Future of Privacy: Positive-Sum NOT Zero-Sum*
2. *The Next Wave: From PETs to PETs Plus, … to Transformative Technologies*
3. *Video Surveillance, Transformed*
4. *Why Privacy is Good for Business*
5. *Managing Your Data*
6. *The New PIA*
7. *Conclusions*

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 a 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 1990's, 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 right 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.

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,

to …

Transformative Technologies

Transformative Technologies

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

<u>Transformative Technology</u>

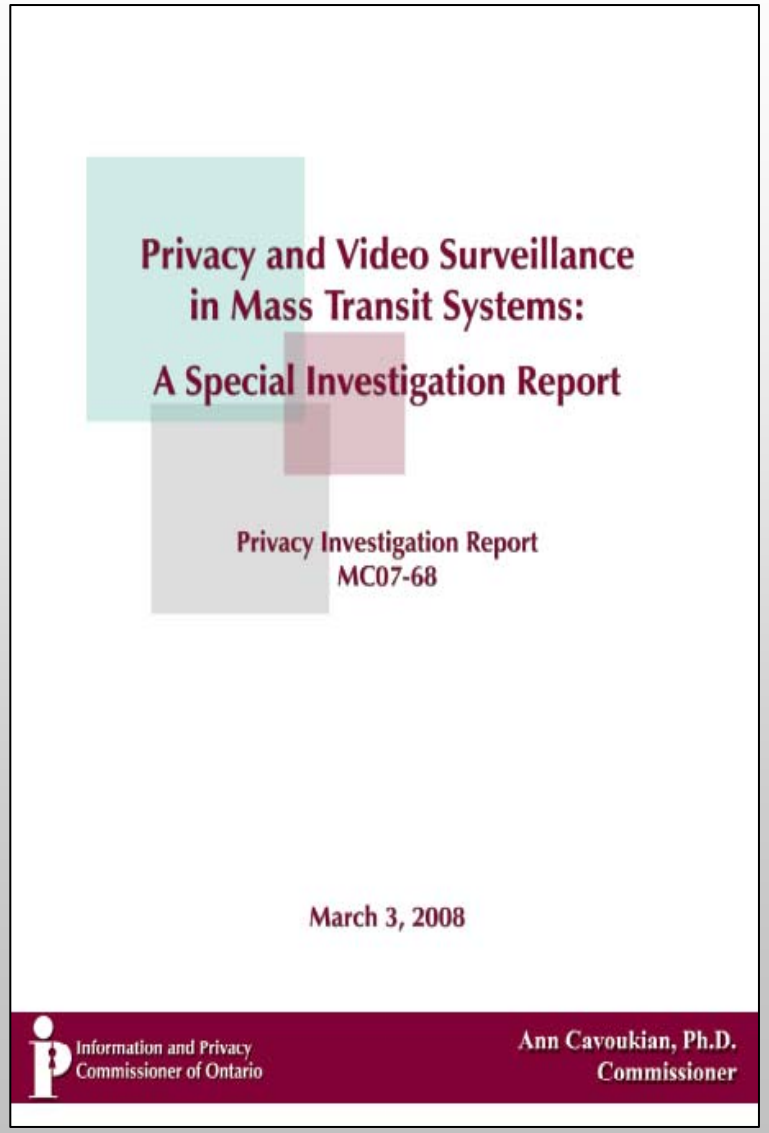
Common characteristics of Transformative Technologies:

- 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.

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).

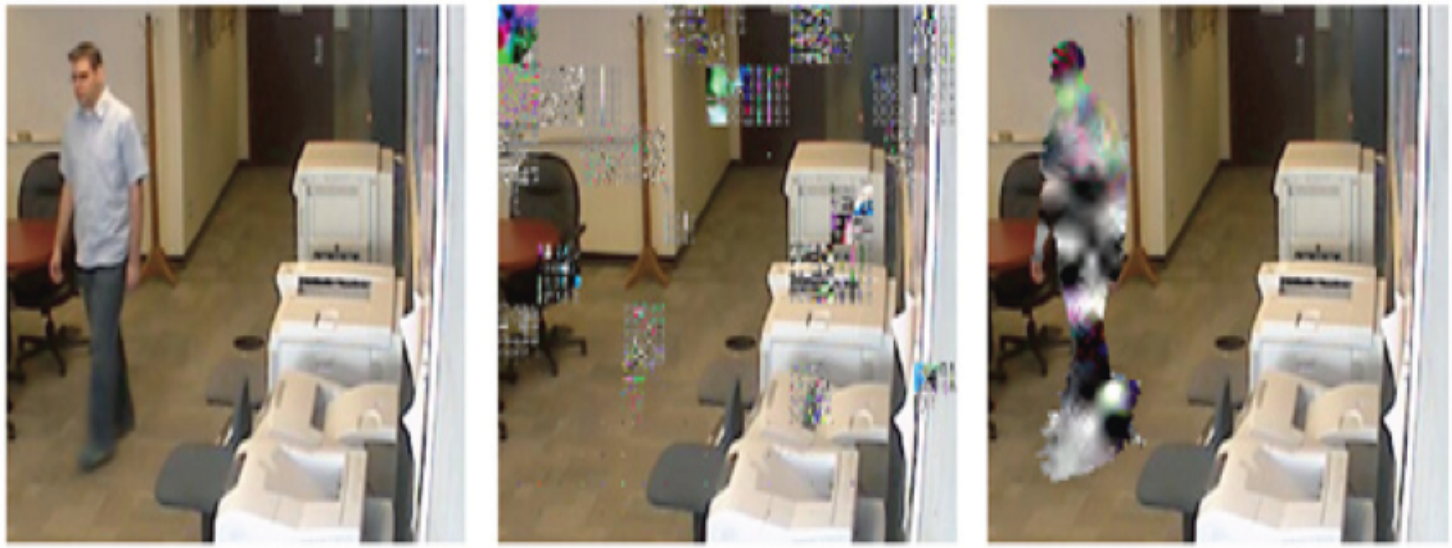


www.ipc.on.ca/images/Findings/mc07-68-ttc.pdf

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

"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

Why Privacy is Good for Business

The Bottom Line

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

Think of privacy as a sound business strategy

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.

Managing Your Data

Managing Your 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?

Assess Your Risks

Assess your risks to privacy:

- Conduct a Privacy Impact Assessment;
- Follow up with independent privacy audits using Generally Accepted Privacy Principles (GAPP). **http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+ Principles/**

The New PIA

A New PIA

- Announcing the launch of a new PIA for use in a Web 2.0 world:

  "**Federated Privacy Impact Assessment (F-PIA)"**

- For use by multiple parties in federated organizations.

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.

www.ipc.on.ca/images/Resources/F-PIA_2.pdf

– 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