Change the Paradigm: Embed Privacy into Technology and Ride the Next Wave

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

Arizona State University
December 3, 2008

Presentation Outline

1. *The Privacy Landscape: Privacy "101"*

2. *Positive-Sum, Not Zero-Sum*

3. *The Next Wave: PETs Plus or Transformative Technologies*

4. *Biometrics Transformed: Biometric Encryption*

5. *Video Surveillance, Transformed*

6. *Radical Pragmatism*

7. *Conclusions*

The Privacy Landscape: Privacy "101"

Privacy = Freedom

Privacy and Security:
The Difference

- Authentication
- Data Integrity
- Confidentiality
- Non-repudiation

Security:

Organizational control of information through information systems

- Privacy; Data Protection
- Fair Information Practices
- "Use" of Personally Identifiable Information (PII)

IPC
www.ipc.on.ca

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."

Fair Information Practices:
A Brief History

- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980);

- European Union Directive on Data Protection (1995/1998);

- CSA Model Code for the Protection of Personal Information (1996);

- United States Safe Harbor Agreement (2000);

- Global Privacy Standard (2006).

  www.ipc.on.ca/images/Resources/up-gps.pdf

Global Privacy Standard

- In 2005, at the 27th International Data Protection Commissioners Conference in Montreux, Switzerland, I chaired a Working Group of Commissioners convened for the sole purpose of creating a single Global Privacy Standard (GPS);

- Globalization and converging business practices created a need to harmonize various sets of fair information practices so that businesses and technology companies could turn to a single instrument for evaluating whether their practices or systems were actually enhancing privacy;

- The GPS builds upon the strengths of existing codes containing time-honoured privacy principles and reflects an enhancement by explicitly recognizing the concept of "data minimization" under the "collection limitation" principle;

- The final version of the GPS was formally tabled and accepted in the United Kingdom, on November 3, 2006, at the 28th International Data Protection Commissioners Conference.

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

IPC
www.ipc.on.ca

Privacy OR Security:
A Zero-Sum Game

Privacy vs. Security
(false dichotomy)

Security

Privacy
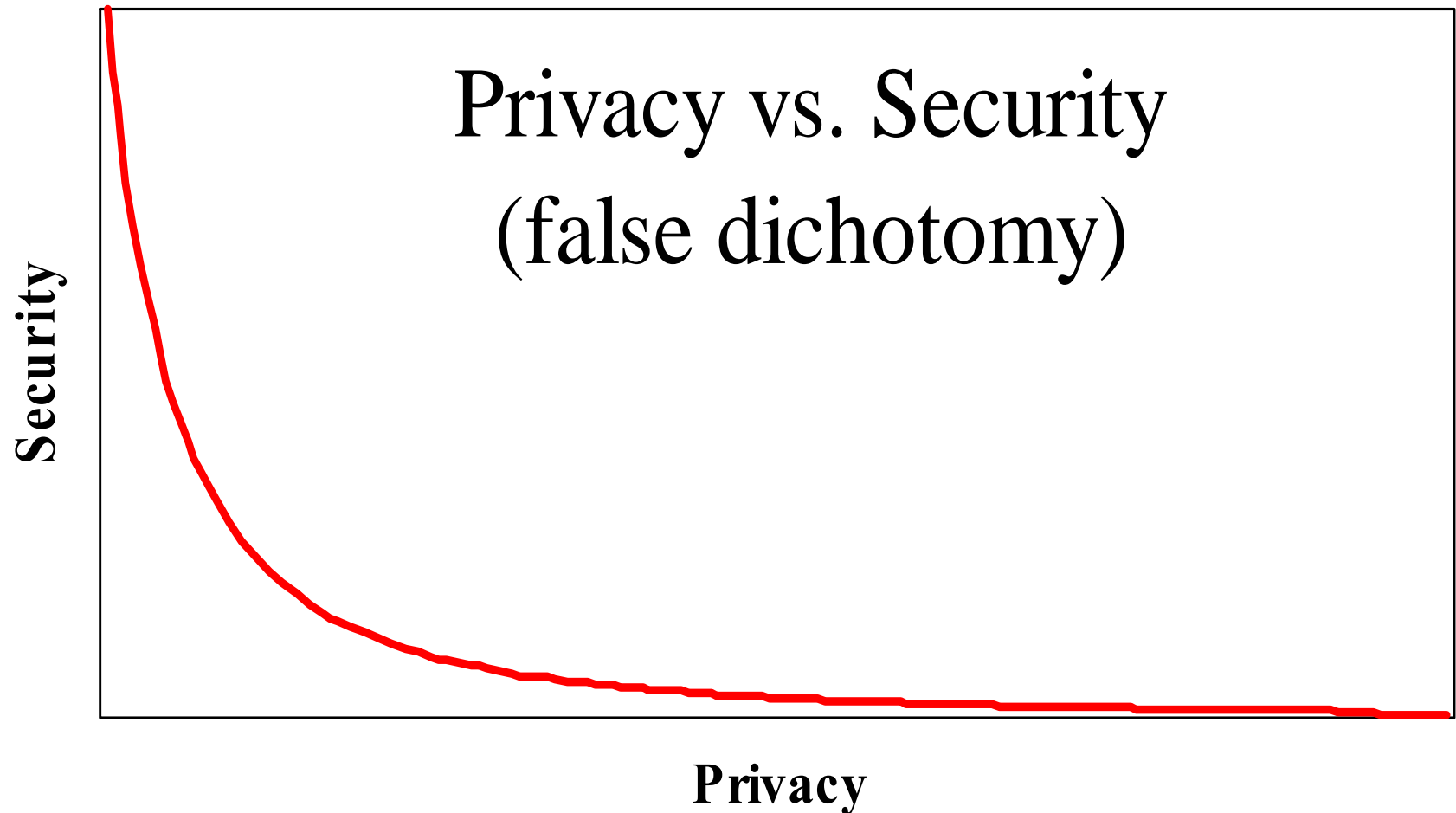
We Need to
Change
The Paradigm

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 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, into the design specifications; into the architecture; embed privacy right into the technology used – *bake it in*;

- Assess the risks to privacy: conduct a privacy impact assessment; follow up with annual privacy audits;

- 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: Transformative Technologies

Time For A Change…

… from PETs to PETs Plus,

or

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.

Biometric Encryption:

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

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

Alex Stoianov, Ph.D.
Biometrics Scientist

February 2007
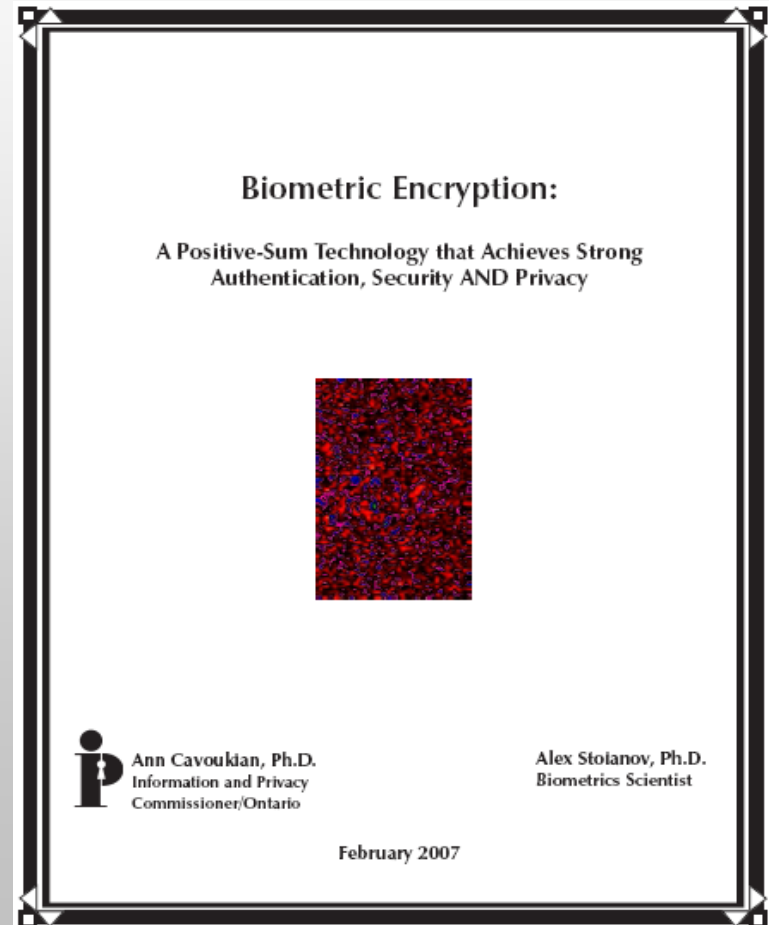
Biometric Encryption (BE)*

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

IPC
www.ipc.on.ca

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.

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).

Privacy and Video Surveillance in Mass Transit Systems:

A Special Investigation Report

Privacy Investigation Report
MC07-68

March 3, 2008

Information and Privacy
Commissioner of Ontario

Ann Cavoukian, Ph.D.
Commissioner

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

IPC
www.ipc.on.ca
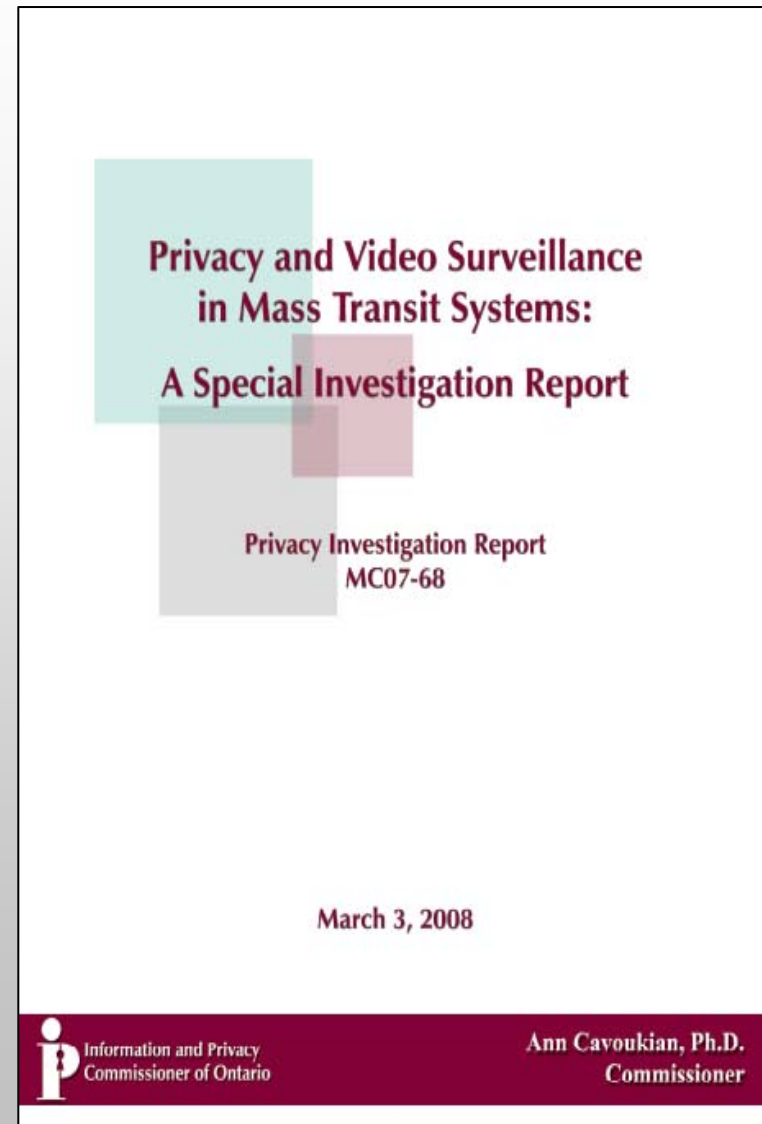
CCTV Cameras:
Innovative Privacy-Enhancing Approach to Video Surveillance

- 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
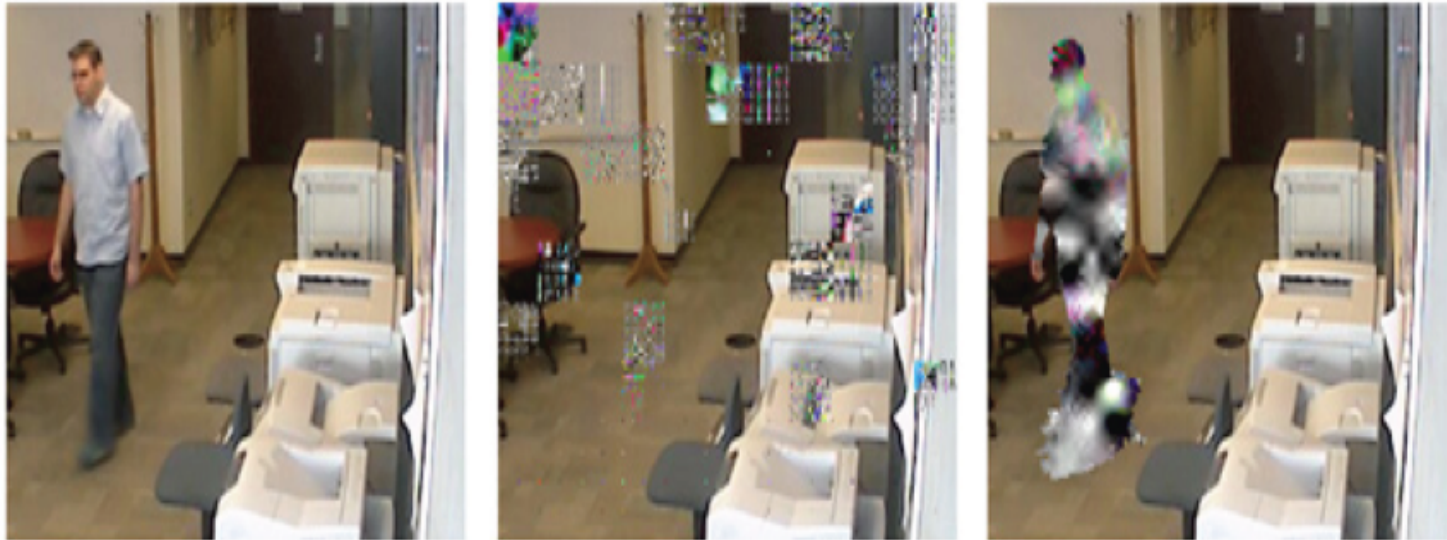
(a)   (b)   (c)

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

Joint Project with RIM

IPC is partnering with RIM (of BlackBerry fame) in association with WeCare Home Health Services, HealthAnywhere (IgeaCare Systems Inc.), and MedShare to ensure a high level of privacy as well as security, relating to the delivery of innovative home healthcare services.

Pragmatism

Radical Pragmatism

Radical

Radical

(/raedikel/ adj, & n.) — adj.

2) **far-reaching … thorough.**

— Concise Oxford Dictionary, Eighth Edition, 1990.

Radical Privacy Pragmatism

Radical = far-reaching … thorough;

Pragmatism ≠ status quo;

Radical Pragmatism (in the area of privacy) is the embodiment of a positive-sum paradigm, involving a practical approach, invoking the need for Transformative Technologies;

Talk – Action = Zero

Identity, Privacy and Security Initiative
University of Toronto

- As we enter into an age immersed in a rich information environment, frequently sharing information about ourselves and others, can privacy remain a viable option?

- Absolutely, but only if we build it in — architecting it directly into technology.

My Challenge to You: How Can You Make a Difference?

Conclusions

- We need to change the paradigm away from a zero-sum game to a positive-sum model where both privacy and security are built directly into technologies;

- The use of privacy-enhancing biometrics such as Biometric Encryption will ensure that privacy is protected, while at the same time, delivering strong security – a true win/win scenario – positive-sum, all the way!

- "Radical pragmatism" reflects an effort to embed privacy protective measures, such as privacy by design, into existing technologies and business practices, in a positive-sum paradigm;

- Work with us to change the paradigm and think differently: We need both privacy AND security, not "either/or."

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