Radical Pragmatism and Transformative Technologies: *The Future of Privacy*

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

The Berlin Group
Strasbourg, France
October 14, 2008

Presentation Outline

1. *Positive-Sum, Not Zero-Sum*
2. *Transformative Technologies*
3. *"Radical Pragmatism"*
4. *Biometrics Transformed*
5. *Conclusions*

2008 or 1984: Fact or Fiction?

"Britain mulls a society in which privacy is banned"

Britain eyes $23B Plan to monitor all e-mail, telephone, Internet records

"The British government is considering a $22.9 billion dollar plan to monitor the e-mail, telephone, and Internet browsing records of every person in the country."

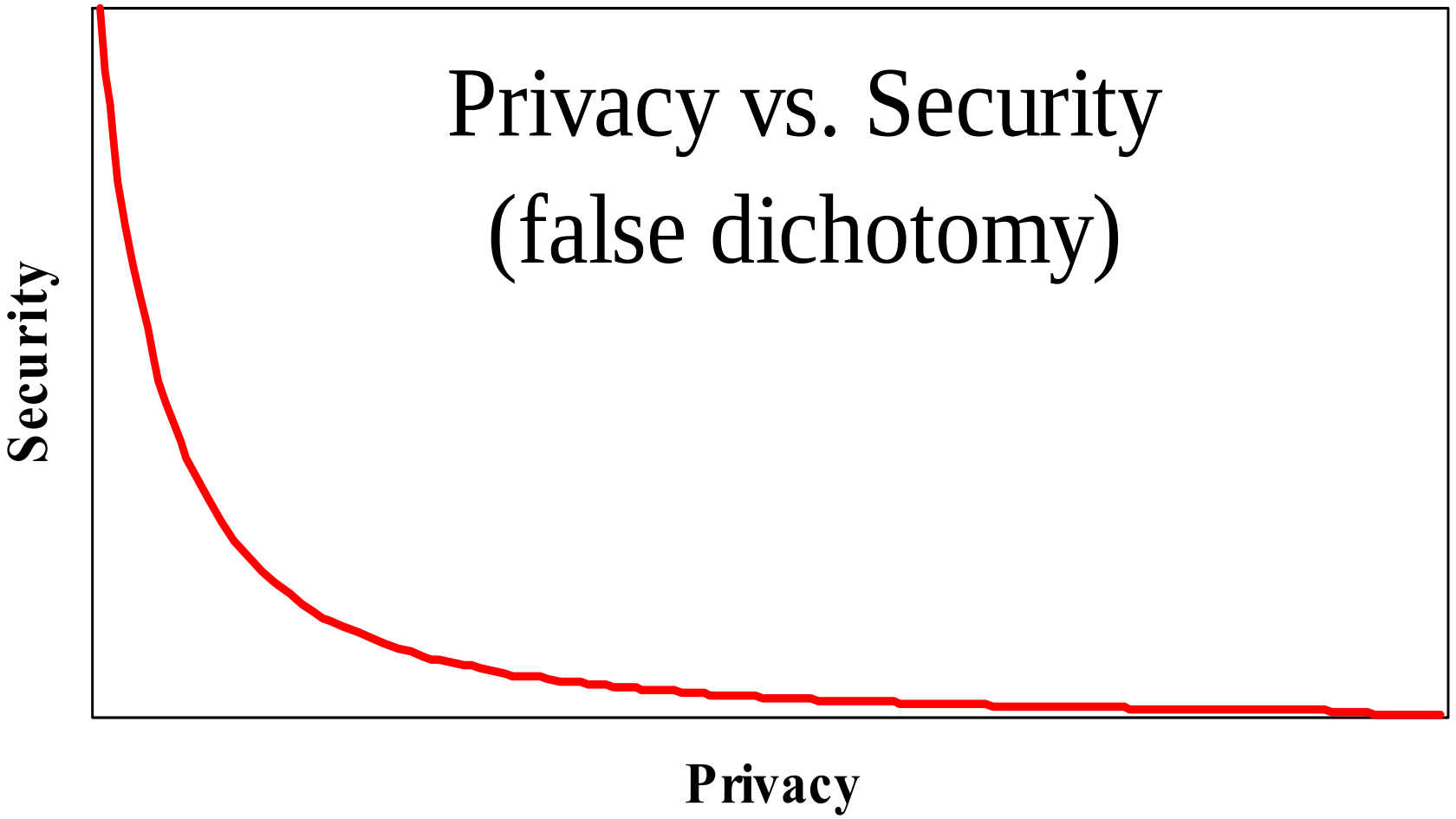
— National Post, October 6, 2008. p. A3.

British Big Brother

"MI5's proposal calls for nothing less than a full-scale surveillance society."

— National Post, October 7, 2008. p. A16.

Privacy OR Security:
A Zero-Sum Game



Positive-Sum
NOT
Zero-Sum

Positive-Sum vs. Zero-Sum

- 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"

- Build in privacy – up front, into the design specifications; into the architecture; if possible 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;

  — **http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+ Principles/**
- 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.

Transformative Technologies

Privacy Invasive Technologies

- There are a growing number of technologies that give rise to a new paradigm of concerns regarding privacy – *especially given the extent of technologies involving surveillance, generally considered to be* ***Privacy Invasive:***
  - Biometric Technologies
  - Radio Frequency Identification (RFID)
  - Video Surveillance Cameras

Apply the Power of Transformative Thinking

- Using transformative thinking, any technology can be architected with privacy built right into its design, reframing it into a **"Transformative Technology."**
- This has been our focus in the numerous joint-projects we have collaborated on, such as:
  - RFID in Health Care
  - Biometric Encryption
  - Mass Transit Surveillance Cameras
  - Identity Management on the Internet
- Concepts such as ***Privacy-Enhancing Technologies (PETs)*** combined with a positive-sum paradigm, can effect transformative change – transforming privacy problems into privacy solutions.

Background: Privacy-Enhancing Technologies *(PETs)*

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

www.ipc.on.ca/images/Resources/anoni-v2.pdf

From PETs to Trans Tech

Do All PETs = Transformative Technologies?

No

Transformative Technologies

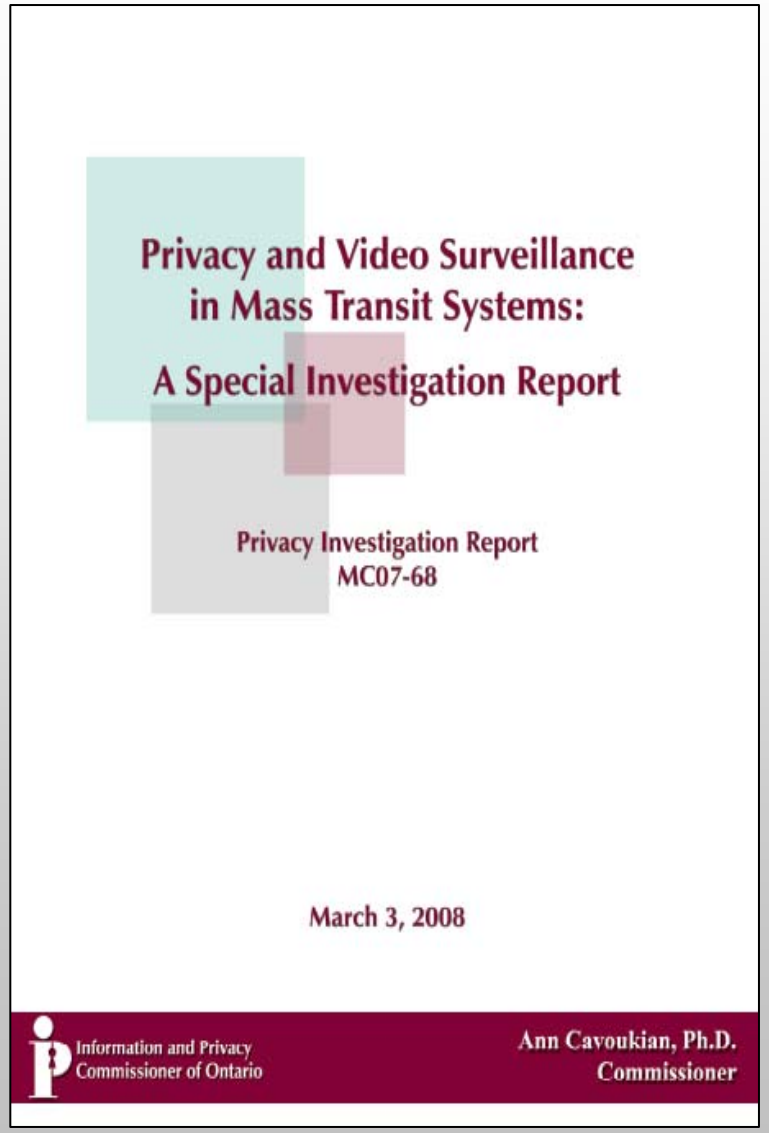
Surveillance Technology + Positive-Sum Paradigm + Privacy Enhancing Technology = Transformative Technologies

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.

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) framework.



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

Pragmatism

Radical
Pragmatism

Radical

Radical

(/raedikel/ adj, & n.) — adj.

2) **far-reaching … thorough.**

— Concise Oxford Dictionary, Eighth Edition, 1990.

Radical "Privacy" Pragmatism

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

Radical Pragmatism

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, often invoking the need for Transformative Technologies;

Talk – Action = Far Less

Biometrics Transformed: Biometric Encryption

European Biometrics Forum

- The European Biometrics Forum (EBF) was launched in 2003 – invited to speak at their inaugural conference in Dublin;
- Asked to become a member of the 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 biometric 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 from 2003-2010.

www.eubiometricforum.com

IPC and Biometrics

- IPC Publication: *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy* (2007)
- EBF IBAC (2005 to present)
- Resolution of International DPAs (2005)
- Statement to House of Commons Standing Committee on Citizenship & Immigration (2003)
- *Ontario Works Act* (1997)
- Biometrics Program, Toronto (1994)

TURBINE

(TrUsted evocable Biometric IdeNtitiEs)

- BE is the focus of a large EU research project, TURBINE (TrUsted evocable Biometric IdeNtitiEs), that is currently being funded by the European Union's (EU) 7th Research and Development Framework Program;
- TURBINE aims to develop biometric identity solutions that combine automatic fingerprint recognition and cryptographic techniques, but its primary objective is to prove that such technologies are commercially viable;
- The EU's funding of TURBINE is a huge endorsement of BE's potential for large-scale applications, and also validation that privacy has a legitimate place in the debate regarding international security regimes.

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.

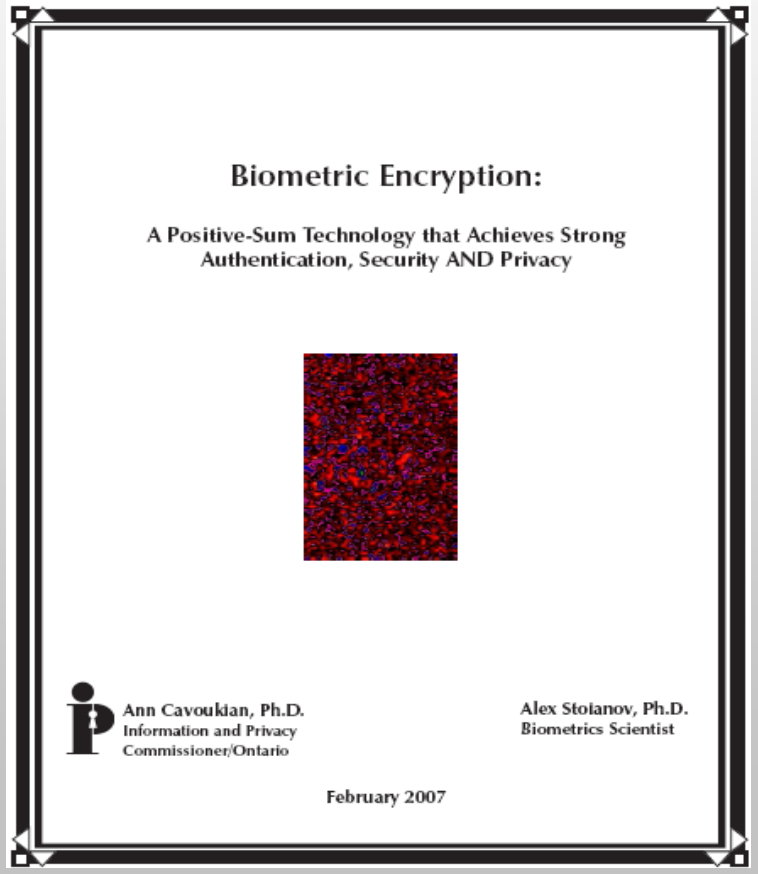
Biometric Encryption (Cont'd)

- 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.

IPC Publication – *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

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.

Dr. Ann Cavoukian

PRIVACY BY DESIGN – "BUILD IT IN"
A CRUCIAL DESIGN PRINCIPLE

Inaugural Lecture of the **Identity, Privacy and Security Initiative (IPSI)**
University of Toronto

What does ubiquitous computing imply for privacy? As we enter into an age where we are 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 the technology. Dr. Cavoukian, Ontario's Information and Privacy Commissioner and the Chair of the University of Toronto's IPSI Advisory Committee, calls this *privacy by design*. Come and hear her explain how this works as she reviews her efforts to shape the evolution of identity technologies, including identity management systems, radio frequency identifiers and biometrics.

The Identity, Privacy and Security Initiative (IPSI) at the University of Toronto is pleased to announce that Dr. Ann Cavoukian will give the inaugural lecture for a new graduate seminar program on September 17, 2007. This seminar links two new graduate concentrations in privacy and security, offered this fall through the Faculty of Applied Science and Engineering and the Faculty of Information Studies. A key goal of the IPS Initiative is to advance the integration of the basic, social and engineering science research required to generate sustainable solutions to privacy and security.

Please Join Us
September 17th, 2007 – 2:00 - 3:00 p.m.
George Ignatieff Theatre, Trinity College
15 Devonshire Place, Toronto, ON

For more information:

Information and Privacy Commissioner/Ontario
(416) 326-3333
www.ipc.on.ca

University of Toronto
IPS Initiative
(416) 946-3076
ipsi@utoronto.ca

www.ipsi.utoronto.ca/site4.aspx

Designing Privacy into Intelligent Agents

"How to Preserve Freedom and Liberty: Design Intelligent Agents to be Smart *and* Respectful of Privacy"

Dr. George Tomko, Ph.D.
Expert-in-Residence

October 6, 2008
Identity, Privacy and Security Initiative
University of Toronto – St. George Campus

Smart Data

Intelligent agents that have been evolved to:

- Protect and secure your personal information;
- disclose your information only when your personal criteria have been met.

— Stay tuned!

Conclusions

- Pragmatism should not be equated with an acceptance of the status quo;
- In the context of privacy, pragmatism reflects the practical need to ensure that measures protective of privacy are woven into the fabric of everyday life;
- Zero-sum paradigms involving privacy juxtaposed against another interest, invariably lead to a loss of privacy;
- BE is an excellent example of a positive-sum technology that delivers both privacy and security – "win/win," not "either/or."
- "Radical pragmatism" reflects an effort to embed privacy protective measures, such as privacy by design, into existing technologies and practices, in a positive-sum paradigm – "win/win," 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