The Future of Privacy Lies in Transformative Technologies:
Positive-Sum, Not Zero-Sum

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

Harvard Executive Privacy Symposium
Harvard University
August 20, 2008

Presentation Outline

1. *Positive-Sum, Not Zero-Sum*
2. *Transformative Technologies*
3. *Video Surveillance, Transformed*
4. *Biometrics Transformed: Biometric Encryption*
5. *ISP Tracking, Transformed*
6. *Radical Pragmatism*
7. *Conclusions*

Positive-Sum
NOT
Zero-Sum

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;
- 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

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.

Pragmatism

Radical
Pragmatism

Radical

Radical

(/raedikel/ adj, & n.) — adj.

2) **far-reaching … thorough.**

— Concise Oxford Dictionary, Eighth Edition, 1990.

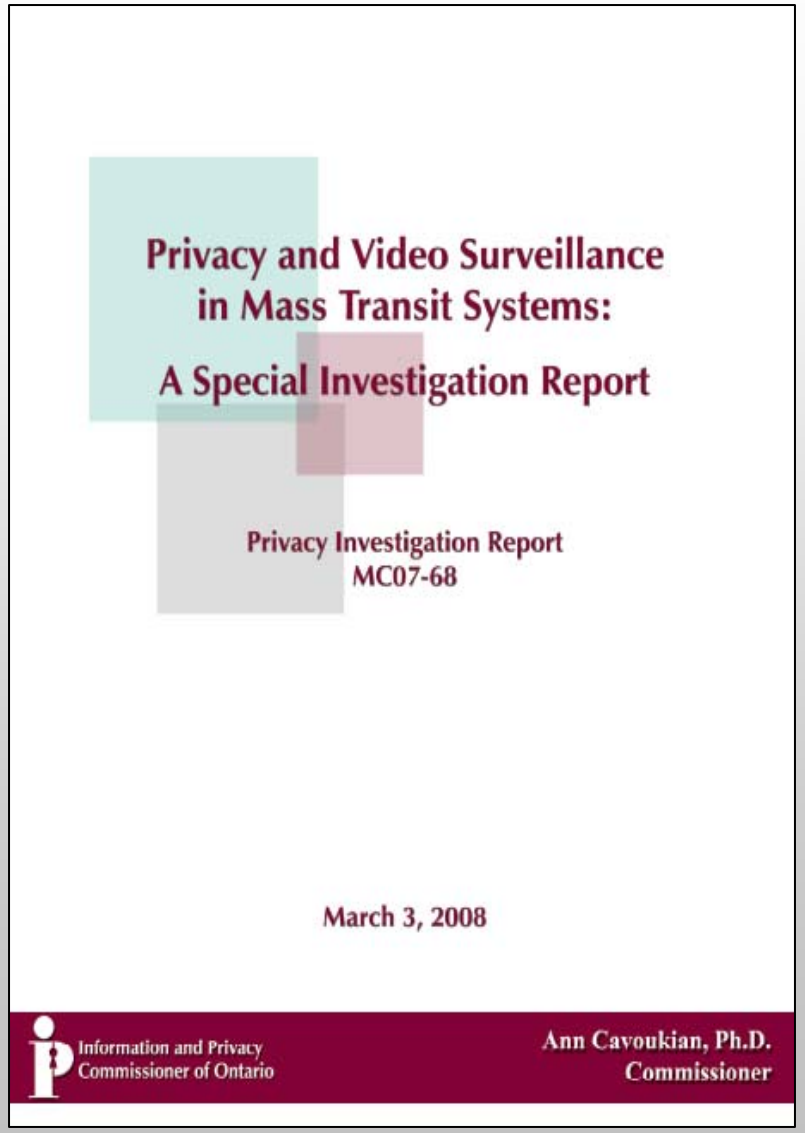
Radical "Privacy" Pragmatism

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

Video Surveillance, Transformed

TTC Surveillance Cameras

- In March 2008, I ruled that the Toronto Transit System's expansion of its video surveillance system, for the purposes of public safety, was in compliance with Ontario's *Municipal Freedom of Information and Protection of Privacy Act.*
- 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;
  - Personal information will only be used and disclosed for the specified purposes.



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

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)

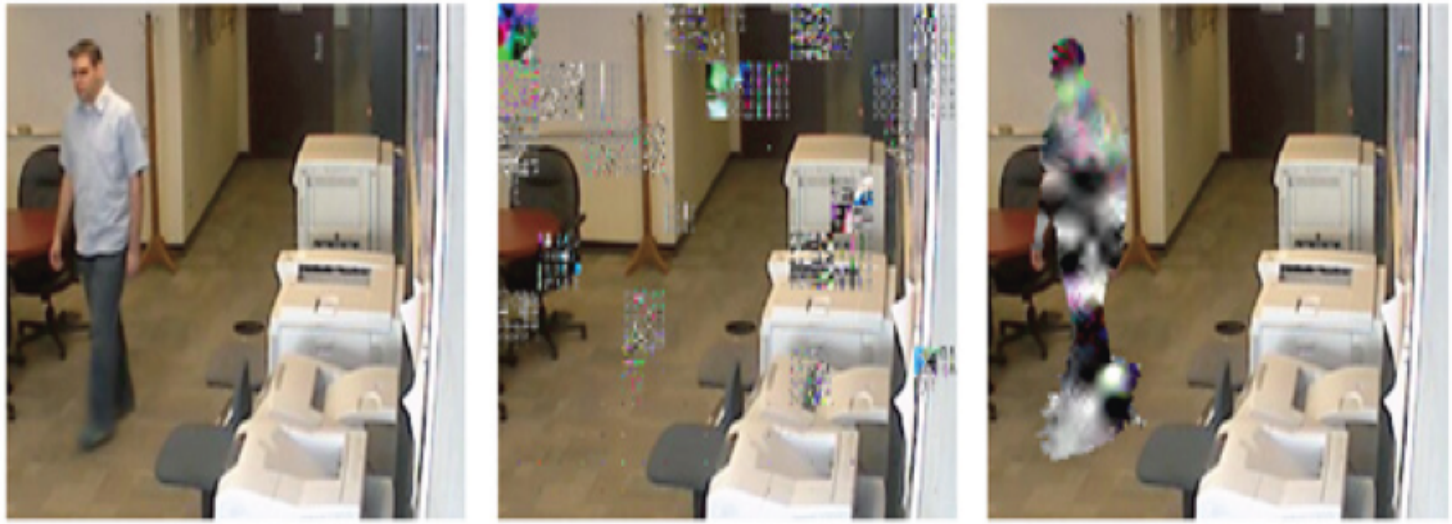
"It sets the bench mark for informed discussion of CCTV in mass transit systems … It provides a roadmap for the most privacy protective approach to CCTV. It offers potential technological solutions that can further enhance privacy with CCTV imagery. It presents specific recommendations and a requirement 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

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; **www.dsp.utoronto.ca/~kmartin/papers/tech_report_2008.01-surveillance**
- 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.

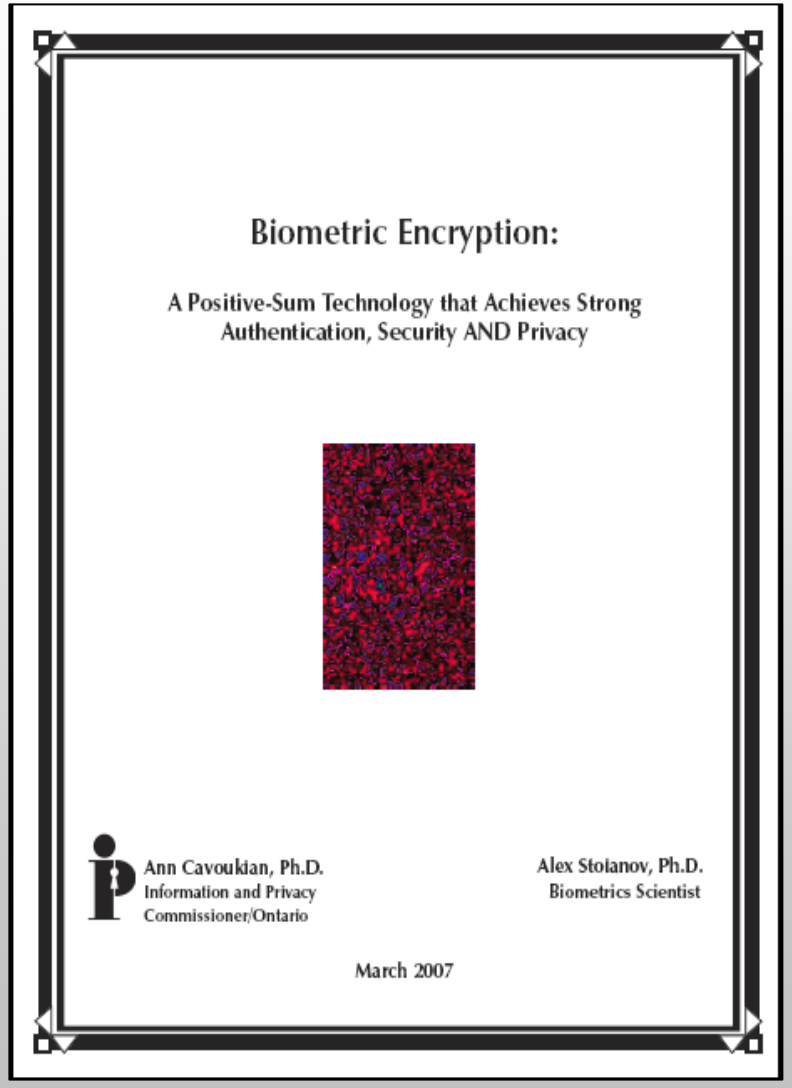
www.ipc.on.ca/images/Findings/mc07-68-ttc_592396093750.pdf

Biometrics Transformed:

Biometric Encryption

IPC Biometrics White Paper

- This paper discusses the privacy-enhanced uses of biometrics, with a particular focus on the privacy and security advantages of Biometric Encryption (BE) – the merits of the BE approach to verifying identity, protecting privacy, and ensuring security;
- The central message is that BE can help to overcome the prevailing "zero-sum" mentality by adding privacy to identification and information systems, resulting in a positive-sum, scenario for all stakeholders.



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

IPSI

Identity, Privacy and Security Initiative

- As we enter into an age immersed in an increasingly 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

ISP Tracking, Transformed

ISP Tracking: Necessary but Risky

- Today's Internet Service Providers (ISPs) need to gather network traces to perform a variety of network management operations such as traffic engineering, capacity planning, threat analysis, and customer accounting;
- Unfortunately, collecting this data can raise significant privacy issues – data can be lost, damaged or stolen, or worse, used to track people's online activities;
- Relying on internal procedures to protect this data is not enough – it does not address insider threats or human error;
- Researchers at the University of Toronto have developed a new technology called **Bunker** that allows ISPs to securely trace their networks, but do so in a privacy-protective manner.

Bunker: Privacy-Protective, Tamper-Resistant Network Tracing*

- "Bunker" automatically creates pre-determined reports:
  - No operator ever handles personally identifiable data (or any data);
- ISPs decide which reports to generate, before the fact – only aggregated data is collected in non-identifiable form;
- "Bunker" stores all data in a tamper-resistant system:
  - If any attempt is made to open the hardware or access the data contained therein, the data will in effect, "self-destruct" – all internal data will be lost upon the attempt to reboot;
  - Limited ability to interact with the system once activated;
- "Bunker" safeguards the privacy of users by:
  - Allowing ISPs to enforce a privacy-protective policy over traces;
  - Preventing insider threats and accidental or wilful disclosure;
  - Decreasing the risk of revealing personally identifiable data upon being served with a subpoena.

**Bunker: Improving the Privacy of Network Tracing with Tamper Resistance*, Professor Stefan Saroiu, Andrew Miklas, et al, University of Toronto, 2008.

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,
involving a practical approach,
often invoking the need for
Transformative Technologies;

Talk – Action = Zero

Conclusions

- Pragmatism should not be equated with an acceptance of the status quo;
- In the context of privacy, it reflects a practical desire to ensure that measures protective of privacy are woven into the fabric of everyday life;
- "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 – "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