Privacy, Technology and Transformation

Ken Anderson
Assistant Commissioner (Privacy)
Ontario

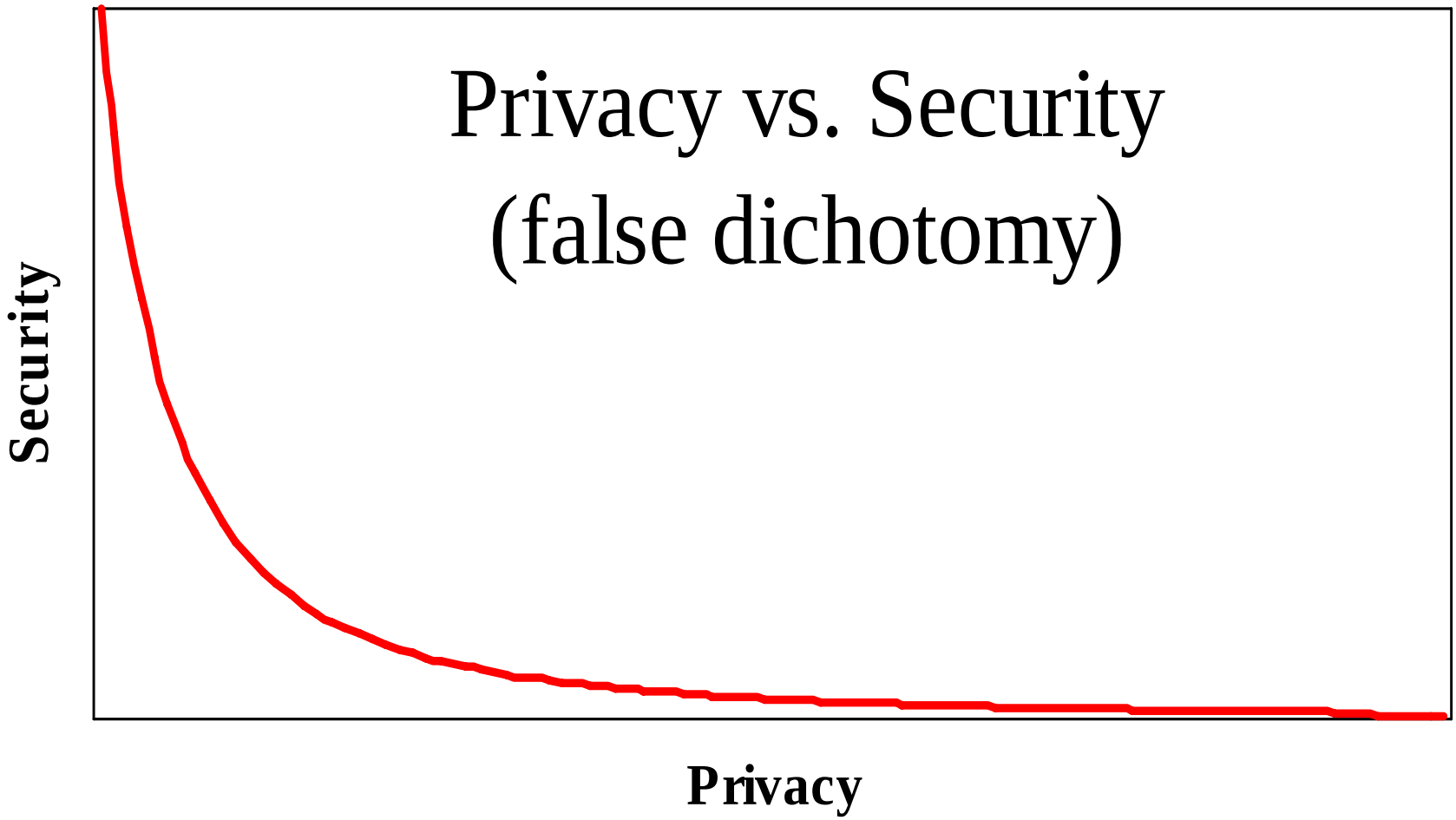
Ontario Shared Services
Information Management and Privacy Forum
June 3, 2008

Presentation Outline

1. *Looking at Privacy Differently*
2. *Transformative Technologies*
3. *Recent IPC Initiatives*
4. *Developing a Culture of Privacy*
5. *Conclusions*

Looking at Privacy Differently

Privacy OR Security:
A Zero-Sum Game



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 trade-offs

Looking at Privacy Differently

Old World: Zero-sum mentality

Future: Positive-sum paradigm

Don't get stuck in the past

Privacy-Enhancing Technologies *(PETs)*

- The IPC developed the concept and methodology recognized around the world today as ***privacy-enhancing technologies*** (PETs);
- PETs include those that empower individuals to manage their own identities in a privacy enhancing manner, such as:
  - anonymizing and pseudonymizing identities;
  - securely managing login IDs and passwords and other authentication requirements;
  - restricting traceability and limit surveillance;
  - allowing users to selectively disclose their Personally Identifiable Information (PII) to others and exert maximum control over their PII once disclosed.

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): give your customers maximum control over their data.

Transformative Technologies

Transformative Technologies

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

Transformative Technologies

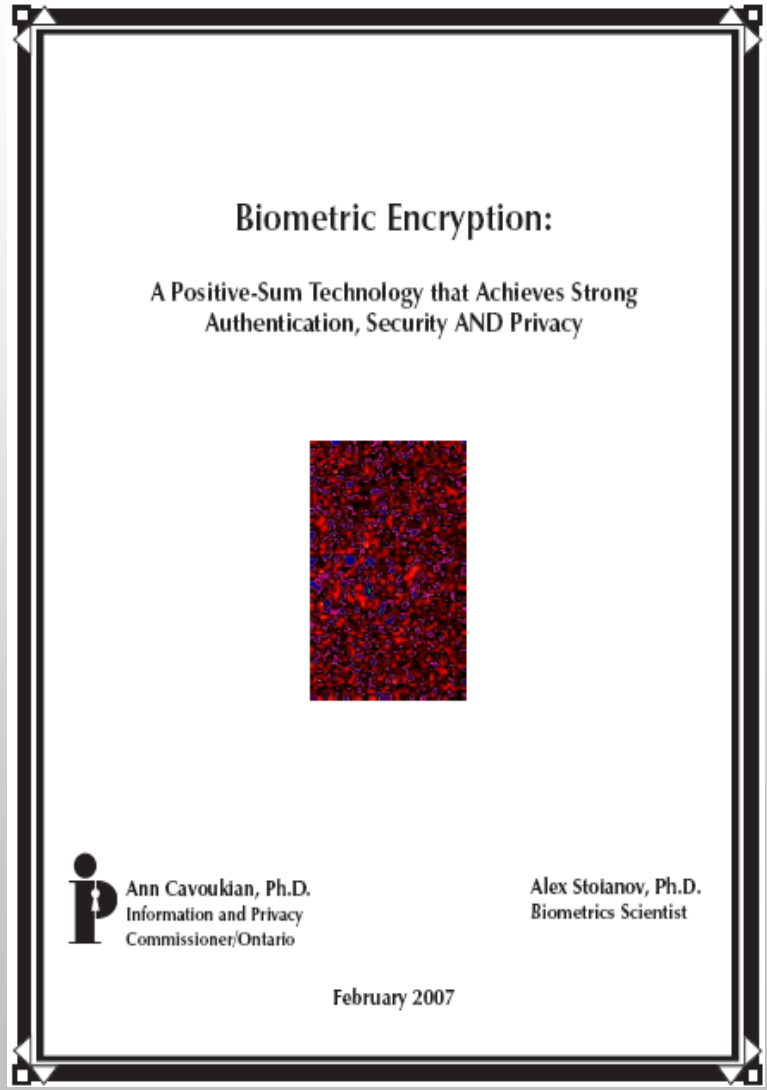
Common characteristics of Transformative Technologies:

- Help minimize unnecessary disclosure, collection, retention and use of personal data;
- Empower individuals to participate in the management of their personal data;
- Enhance the security of personal data, if collected/used;
- Promote public confidence and trust in (personal) data governance structures;
- Help promote and facilitate widespread adoption of those technologies.

Recent IPC Initiatives

IPC Biometrics White Paper

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



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

Ontario Lottery Gaming Corp.

Self-Exclusion Program

- The Ontario Lottery and Gaming Corporation (OLG) is exploring the use of facial biometrics to assist Ontarians who voluntarily choose to provide photos of themselves so that they can be denied entry into casinos because of their gambling addiction;
- Any technology solution that the OLG considers will need to be cost-effective, able to detect self-identified gamblers, not interfere with the smooth flow of other patrons into the casino, and respect **all** casino patrons' privacy;
- In undertaking their research on facial recognition technology, OLG has agreed that the application of BE to the solution they choose will be a win-win not, just for the self-identified gamblers, but also to ensure the privacy of all casino patrons.

University of Toronto and the Ontario Lottery Gaming Corporation

- The University of Toronto is undertaking the necessary research to develop a “made in Ontario” BE solution that can be integrated with facial recognition technology;
- When the lab work is completed, we believe this BE solution will lead to a commercially viable product that will garner considerable acclaim for Ontario and Canada;
- The OLG’s support of this BE research and product development is a demonstration of responsible public management with respect to gaming and privacy protection.

Enhanced Driver's Licenses

Non-negotiable requirements as set out by U.S. Department of Homeland Security (DHS) – **Citizenship and RFID Technology**.

Privacy Issues:

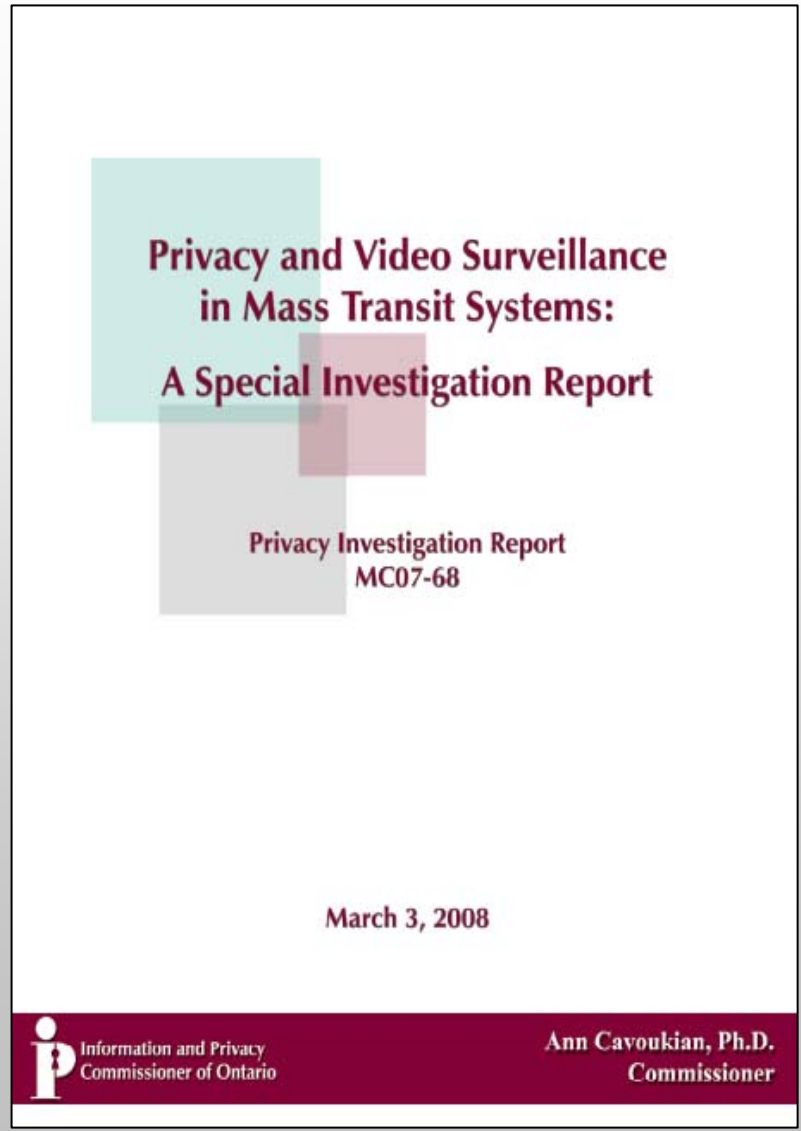
- DHS recommended that Canadian data reside on their border servers;
- Security of RFID technology;
- Citizenship certificate process;

Current Status:

- Privacy Impact Assessment (PIA) process;
- Issue with Canadian Border Services Agency (CBSA) regarding the storage of EDL data by the CBSA and the need for conforming to Canadian and provincial privacy laws – **data to stay in Canada**;
- IPC initiated dialogue with the federal Ministry of Public Safety and the Ontario Deputy Ministers of Transportation and Intergovernmental Affairs regarding duplication of citizenship databases between federal and provincial governments.

TTC Surveillance Cameras

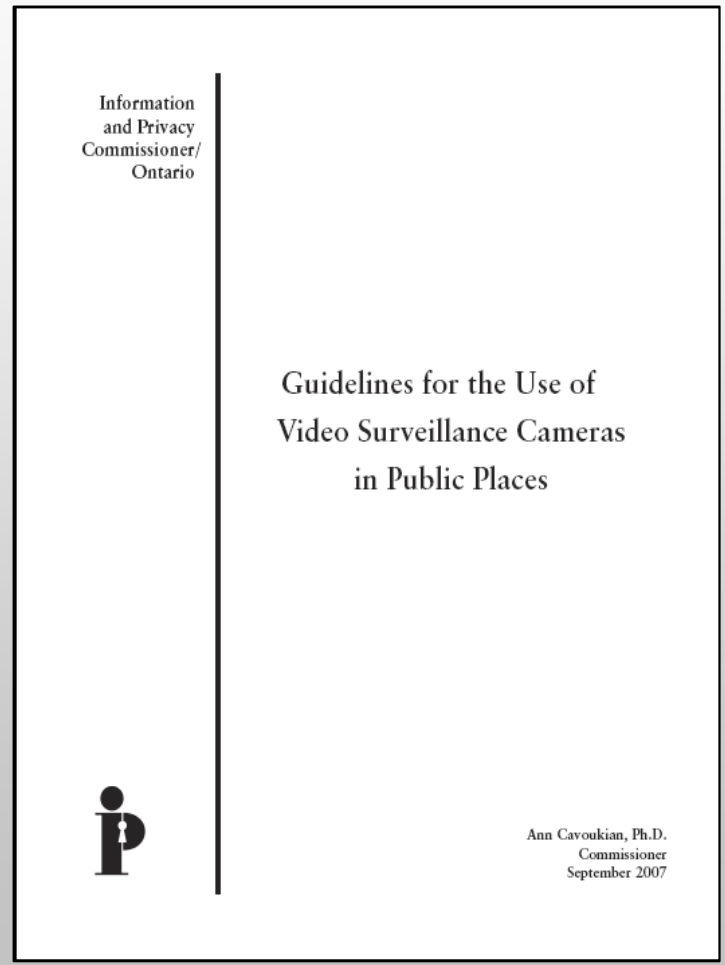
- In March 2008, I ruled that the Toronto Transit System's expansion of its video surveillance system, for the purposes of public safety, was in compliance with Ontario's *Municipal Freedom of Information and Protection of Privacy Act.*
- However, I called upon the TTC to undertake a number of specific 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

IPC Guidelines for the Use of Video Surveillance Cameras in Public Places

- Collection of Personal Information Using a Video Surveillance System;
- Considerations Prior to Using a Video Surveillance System;
- Developing the Policy for a Video Surveillance System;
- Designing and Installing Video Surveillance Equipment;
- Access, Use, Disclosure, Retention, Security and Disposal of Video Surveillance Records;
- Auditing and Evaluating the Use of a Video Surveillance System.



www.ipc.on.ca/images/Resources/up-3video_e_sep07.pdf

Adoption Ruling

March 2005:

- I spoke out against the adoption disclosure Bill 183, *Adoption Information Disclosure Act*, stating that the proposed law needed an amendment giving birth parents and adoptees from adoptions that occurred prior to the passing of this retroactive law the right, if desired, to file a disclosure veto to prevent the opening of their sealed files;
- Nevertheless, the *Act* received Royal Assent without my proposed disclosure veto.

September 2007:

- The Ontario Superior Court of Justice ruled the *Act* as unconstitutional – breaching section 7 of the *Canadian Charter of Rights and Freedoms* and thus, the sections of the *Act* relating to access to birth registration information were invalid.

November 2007:

- The government of Ontario introduced new adoption legislation that includes both a disclosure veto for adoptees and birth parents in adoptions that have already taken place and also promotes openness for adoptions where a disclosure veto is not registered and for all future adoptions.

May 2008:

- The *Access to Adoption Records Act (Vital Statistics Statute Law Amendment)* is now enacted!

Developing A Culture of Privacy

Building A Culture of Privacy

- A culture of privacy enables sustained collective action by providing people with a similarity of approach, outlook, and priorities;
- ***The critical importance of privacy must be a message that comes straight from the top;***
- Privacy must be woven into the fabric of the day-to-day operations of an organization, with adequate resources.

The OSS Example

- IPC and OSS (2004);
- OSS-Deloitte Privacy Review (2005);
- OSS Focus on Privacy (2008).

Kudos to …

- David Hallett, Associate Deputy Manager
- Estella Cohen, Manager
- David Jackson, Privacy Advisor
- Valentina Stankovic, Privacy Advisor

The OSS Example (Cont'd)

- OSS took the Deloitte report with its several hundred questions and made it their own by collapsing the questions to a manageable number, using it as a framework for undertaking internal privacy audits – Bravo!
- Super Clean Days;
- Privacy metrics incorporated into performance plans of senior management;
- Made May "Privacy Awareness Month" for OSS;
- Continuing Privacy displays at Town Halls (e.g. GTA, Orillia and Peterborough);
- Lunch 'n' Learn ID theft sessions;
- 2-hour privacy awareness sessions in the GTA and Resource Exhibit;
- Privacy related e-communications to OSS staff.

IPC Philosophy
The 3 C's

- **Consultation**: by keeping open lines of communication
- **Co-operation**: rather than confrontation in resolving complaints
- **Collaboration**: through working together to find solutions

Conclusions

- Co-operative – 3 C's;
- Bravo OSS for being a privacy role model – now let's roll it out to the rest of the Ontario public sector;
- OSS will now serve a positive example and benchmark for other public sector organizations.

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