Privacy and Digital Identity:
Implications For The Internet

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

Identity in the Information Society Workshop
Lake Maggiore, Italy
May 28, 2008

Presentation Outline

1. *What Privacy is Not*
2. *Transformative Technologies*
3. *Privacy from Web 2.0 to Web 3.0*
4. *The Identity Management Space*
5. *Privacy in the Clouds*
6. *Call for Privacy Advancing Systems*
7. *How do we get there?*
8. *Conclusions*

What Privacy is Not

Privacy Defined

Informational 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."

What Privacy is Not

Privacy ≠ Security

Privacy and Security:
The Difference

Security =

- Authentication
- Data Integrity
- Confidentiality
- Non-repudiation

} Organizational control of information through information systems

Privacy/Data Protection = personal control involving:

Fair Information Practices/Global Privacy Standard

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

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

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
  - Identity Management

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)*** 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

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 independent privacy audits using GAPP – **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): give your customers maximum control over their data.

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 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 to promote and facilitate widespread adoption of transformative technologies.

Let's Change the Way We Look at Privacy and Security

Old World: Zero-sum mentality

Future: Positive-sum paradigm

Don't get stuck in the past

Privacy from Web 2.0 to Web 3.0

Context:
Web 2.0 and Beyond (Web 3.0)

- Unlimited PII creation, sharing and uses online;
- Architectures of participation;
- Decentralization and modularity;
- Collective intelligence …

  But who controls the data?

- **Web 3.0?** – The seamless merger of real-world and web-based data interactions.

Why Privacy is an Issue in Web 2.0 and 3.0

- Authentication vs. Identification;
- Data minimization, if possible;
- User in control vs. user not directly in control;
- Transparency/accountability/governance;
- Widespread use of biometrics.

The Identity Management Space

Building User-Centric Privacy into an Identity Metasystem

- The emergence of an Identity Metasystem is a profound development – there has never been a more strategic time to ensure that privacy interests are built into the new architecture of identity;
- Supporters of Kim Cameron's 7 Laws of Identity and the Identity Metasystem call this the "Identity Big Bang" that will enable ubiquitous intelligent services and a true marketplace *(Web 2.0)* for portable identities;
- Since we noticed many parallels between the 7 Laws of Identity and Fair Information Practices, the two sets of principles being fundamentally complementary, we decided to embed privacy directly into them.

The "Privacy-Embedded" 7 Laws of Identity

1. **Personal Control and Consent:**
2. **Minimal Disclosure For Limited Use: Data Minimization**
3. **Justifiable Parties: "Need To Know" Access**
4. **Directed Identity: Protection and Accountability**
5. **Pluralism of Operators and Technologies: Minimizing Surveillance**
6. **The Human Face: Understanding Is Key**
7. **Consistent Experience Across Contexts: Enhanced User Empowerment And Control**

Implications for Users

The Privacy-Embedded 7 Laws of Identity offer:

- Easier and more direct control over one's personal information when online;
- Embedded ability to minimize the amount of identifying data revealed online;
- Embedded ability to minimize the linkage between different identities and online activities;
- Embedded ability to detect fraudulent email messages and fake web sites (less spam, phishing, pharming, online fraud).

Privacy in the Clouds

Privacy in the Clouds

Evolution of Consumer Computing:

1. **The stand-alone PC** in which the user's software and data are stored on a single, easily protected machine, such as word processing, spreadsheets;

2. **The Web** in which most of the software a user needs is still on their own PC, but more and more of the data they need is found on the Internet, such as a Web browser;

3. **The "Cloud"** in which users rely heavily on data and software that reside externally on the Internet. Examples: using Google Apps for word-processing; virtual worlds such as Second Life that enable users to build 3D environments combining Web pages and Web applications.

   See *The Information Factories* by George Gilder, Wired magazine, October, 2006, www.wired.com/wired/archive/14.10/cloudware_pr.html

Digital Identity Today

- Almost all online activities, such as sending emails, filing tax declarations, managing bank accounts, buying goods, playing games, connecting to a company intranet, and meeting people in a virtual world, require users to establish their identity **each time** they use a new application, usually by filling out an online form and providing sensitive personal information;

- If you count cookies and IP addresses as personal information, then Internet users can leave behind their personally identifiable information everywhere they go **– digital bread crumbs –** and they have little idea how that data may be used or distorted.

The Power and the Promise of Cloud Computing

- **Limitless flexibility**: With access to millions of different pieces of software and databases, and the ability to combine them into customized services, users are better able to find the answers they need, to share their ideas, and enjoy online games, video, and virtual worlds;
- **Better reliability and security**: Users no longer have to worry about their hard drives crashing or their laptops being stolen;
- **Enhanced collaboration**: By enabling online sharing of information and applications, the Cloud offers users new ways of working and "playing" together (think social networks);
- **Portability**: Users can access their data and tools anywhere that they can connect to the Internet;
- **Simpler devices**: With data and the software being stored in the Cloud, users no longer need a powerful computer. They can interface using a cell phone, a PDA, a personal video recorder, an online game console, their cars, or even sensors build into their clothing.

The Digital Identity Needs of Tomorrow

- What is needed – ***flexible*** and ***user-centric*** identity management:
- ***Flexible*** to support the multitude of identity mechanisms and protocols that exist and are still emerging, and the different types of platforms, applications and service-oriented architectural patterns in use;
- ***User-Centric*** because end users are at the core of identity management – they must be empowered to execute effective controls over their personal information;
- A truly flexible identity management system would not be limited to laptop and desktop computers; it would also work on cell phones, PDAs, consumer electronics like video recorders and online game consoles — any way a user might touch the Internet.

Identity Service Requirements in the Cloud

Cloud computing requires identity services that:

- Are device independent;
- Enable a single sign-on to thousands of online services;
- Allow pseudonyms and multiple discrete (and valid) identities to protect user privacy;
- Are interoperable, based on open standards, and available in open source software (to maximize user choice);
- Enable federated identity management; and
- Are transparent and lend themselves to audit.

Call for Privacy Advancing Systems

Cloud Technology Building Blocks

1. **Open source and proprietary identity software based on open standards,** which can be easily incorporated into the full range of online services;

2. **Federated identity** so that once users have authenticated themselves with one service or institution, their identity credentials will be recognized elsewhere. Brokering of security and authentication will eliminate the need to use a different stand-alone log-on process for each application or online service – resulting in significant gains for users;

Cloud Technology Building Blocks (Cont'd)

3. **Multiple and partial identities** so that a user can access online services, explore virtual worlds, and collaborate with others without necessarily revealing their real name and identity to everyone. Different pseudonyms should support differing ranges of identification and authentication strengths;

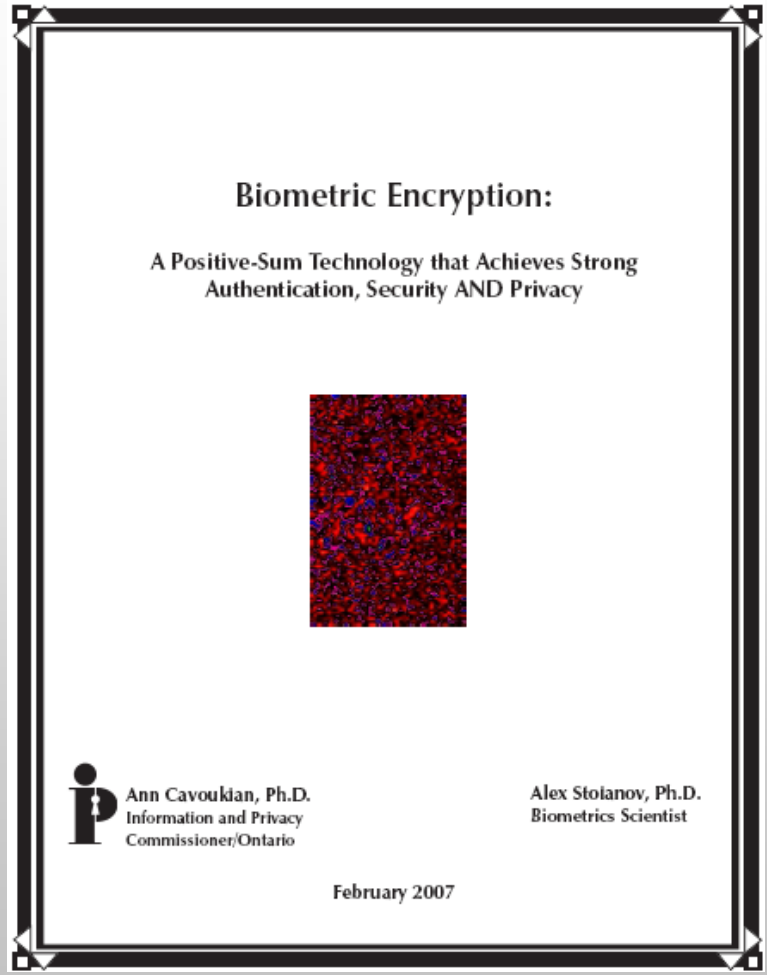
4. **Data-centred policies** that are generated when a user provides personal information and which travel with the information throughout its lifetime to ensure the information is used only in accordance with the rules;

5. **Audit tools** so users can easily determine how their data is being stored, protected, and used, and find out if the policies have been properly enforced.

How do we get there?

IPC Paper on BE

- Privacy-enhanced uses of biometrics, with a particular focus on the privacy and security advantages of Biometric Encryption (BE);
- Engage a broad audience to consider the merits of the BE approach to verifying identity, protecting privacy, and ensuring security;
- 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.

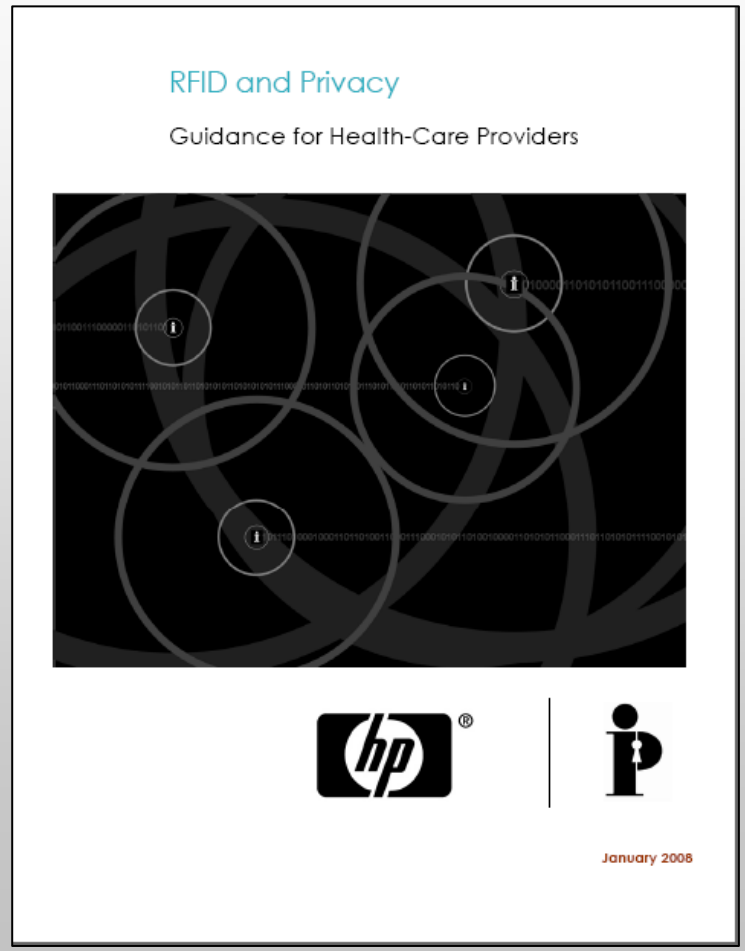


www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf

RFID and Privacy in Health Care:
Guidance for Health Care Providers

- This paper is organized into three broad categories according to the increasing level of potential risk to privacy:

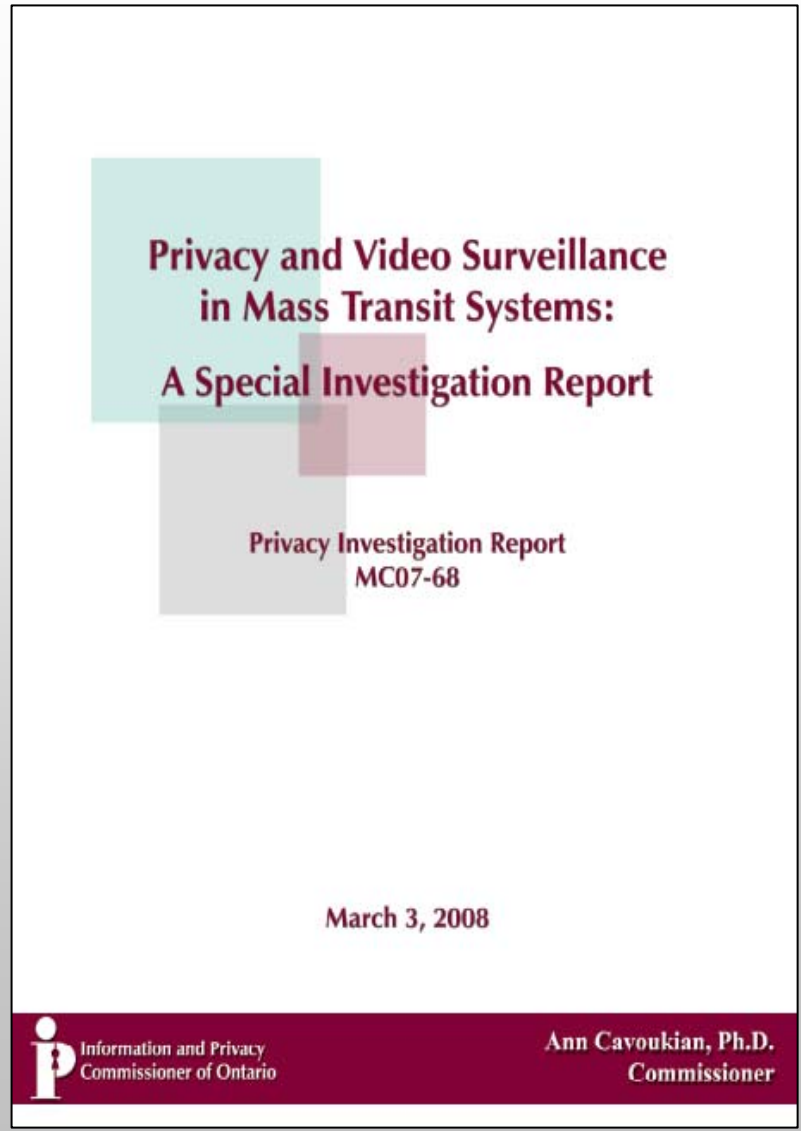
1. **RFID technology used to track things alone;**
2. **RFID technology used to track things associated with people; and**
3. **RFID technology used to track people.**



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

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.

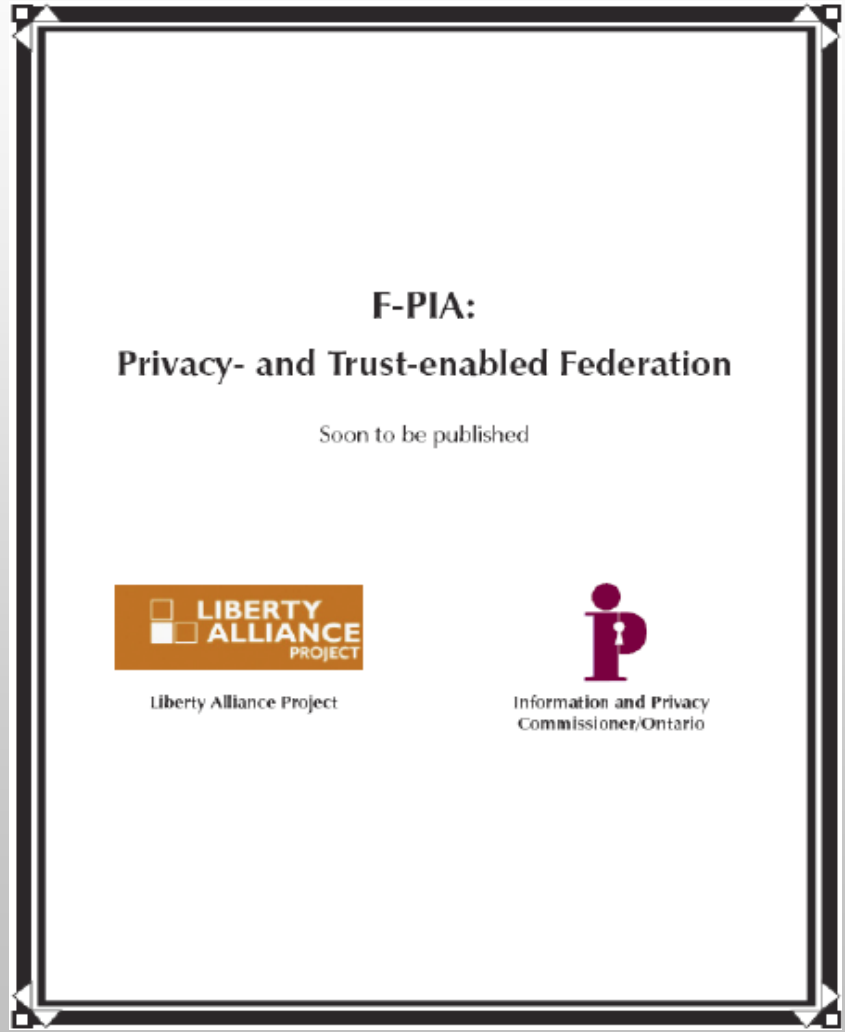


www.ipc.on.ca/images/Findings/mc07-68-ttc.pdf

F-PIA
Privacy and Trust Enabled Federation

Federated Identity Management – Privacy Impact Assessment

The IPC is working with Liberty Alliance through Joseph H. Alhadeff, Chief Privacy Officer for Oracle Corporation, on a Privacy Impact Assessment tool for Federated Identity Systems.



www.ipc.on.ca

Conclusions

Transforming Web 2.0 Technologies of Identity:

What you need to do …

Preserve and promote user privacy through:

- Enhanced user controls;
- Data minimization;
- Improved safeguards.

Develop user-centric identity technologies that are:

- Interoperable and easy to use;
- Based upon free and open standards;
- Trustworthy and accountable.

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