# *Building Privacy into Cloud Computing*

**Ken Anderson**

**Assistant Commissioner (Privacy)**
**Ontario**

**IT 360° Conference & Expo**
**Toronto, Ontario**
***April 07, 2010***

# Presentation Outline

1. *Web 2.0 and beyond*
2. *The Power and the Promise of Cloud Computing*
3. *Identity Service Requirements in the Cloud*
4. *Digital Identity Needs of Tomorrow*
5. *A Call to Action*
6. *Conclusions*

# Who We Are

## Commissioner Ann Cavoukian, Ph.D.

- appointed by Ontario legislature
- independent from government
- oversees 3 privacy & access to information laws

## Mandated to:

- investigate privacy complaints
- resolve appeals from refusals to provide access to information
- ensure organizations comply with access and privacy provisions of the *Acts*
- educate public about Ontario's access and privacy laws
- conduct research on access and privacy issues, provide advice and comment on proposed government legislation & programs.

# Key Definitions

- **Information privacy** refers to the right or ability of individuals to exercise control over the collection, use and disclosure by others of their personal information
- **Personally-identifiable information (“PII”)** can be biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational or reputational, and is the stuff that makes up our modern identity

*Personal information must be managed responsibly. When it is not, accountability is undermined and confidence in our evolving information society is eroded.*

# Applying Privacy to Information Systems

- **Minimize collection, use, sharing, and retention of PII**
  (*e.g.*, limiting purposes, collection, use, disclosure, and retention)

- **Enhance data security**
  (*e.g.*, appropriate safeguards)

- **Actively engage the individual in managing and controlling their PII**
  (*e.g.*, consent, accuracy, access, challenging compliance, etc.)

# 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

**Information Privacy = *personal* control**

# Privacy-Enhancing Technologies

- **Privacy-Enhancing Technologies (PETs)** embody the *Fair Information Practices*
- **PETs *Plus***
  www.ipc.on.ca/images/Resources/petsplus_3.pdf
- **Positive-Sum Approach & Results**
  *Privacy & Radical Pragmatism: Change the Paradigm* (2008)
  www.ipc.on.ca/images/Resources/radicalpragmatism_752070343750.pdf
- ***Transformative* Technologies** change the paradigm from a zero-sum to a positive-sum model. Create “win-win” scenarios not “either/or” involving trade-offs and false dichotomies

  *Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum not Zero-Sum* (2008):
  www.ipc.on.ca/images/Resources/trans-tech-handout_1.pdf

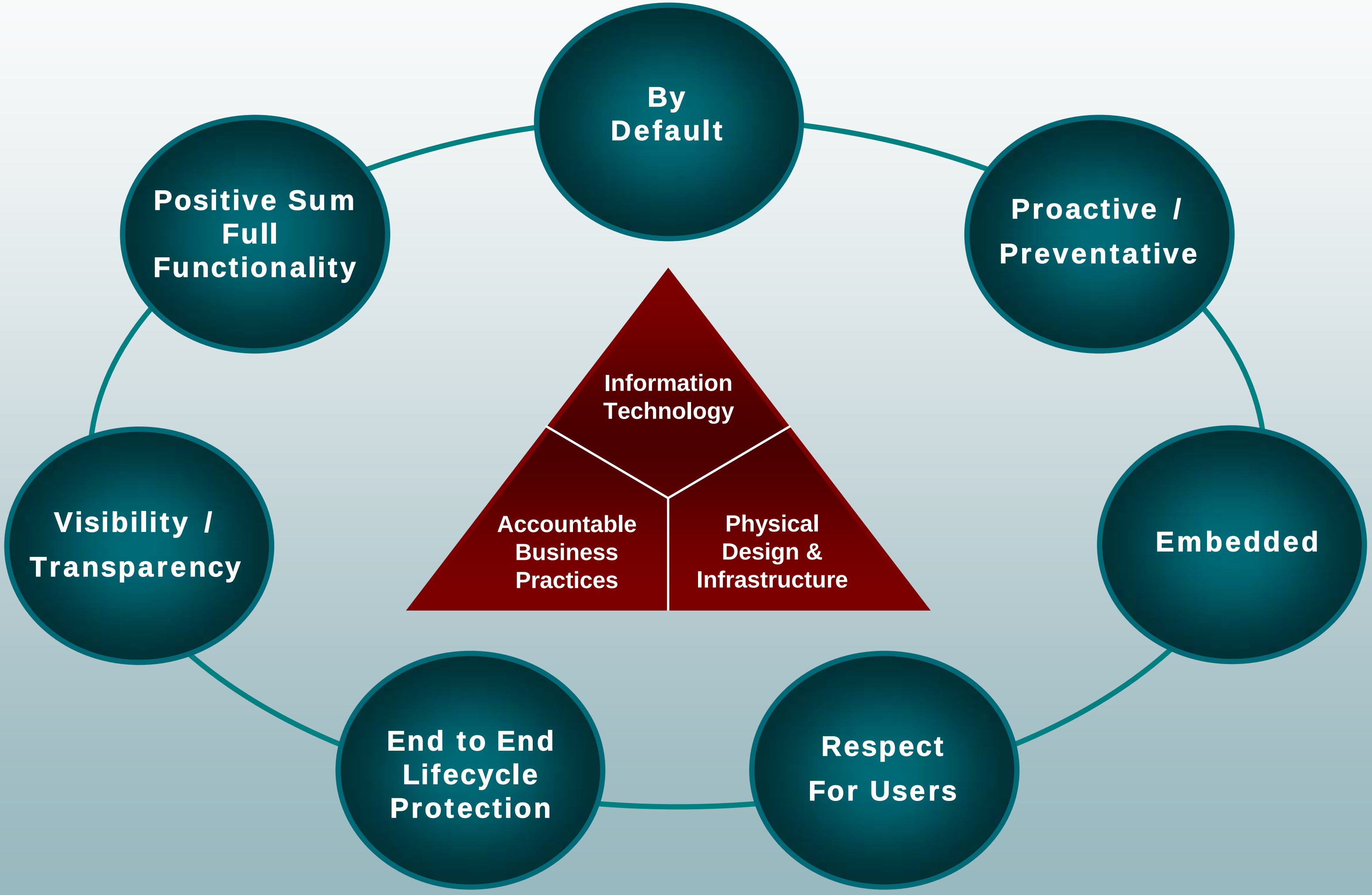
# Privacy by Design: “Build It In”

## Key elements:

1. Privacy interests and concerns must be addressed
2. Mitigate privacy concerns early when developing information technologies and systems
3. Apply basic principles expressing universal privacy protection
4. Qualified privacy leadership and/or professional input
5. Adopt and integrate privacy-enhancing technologies

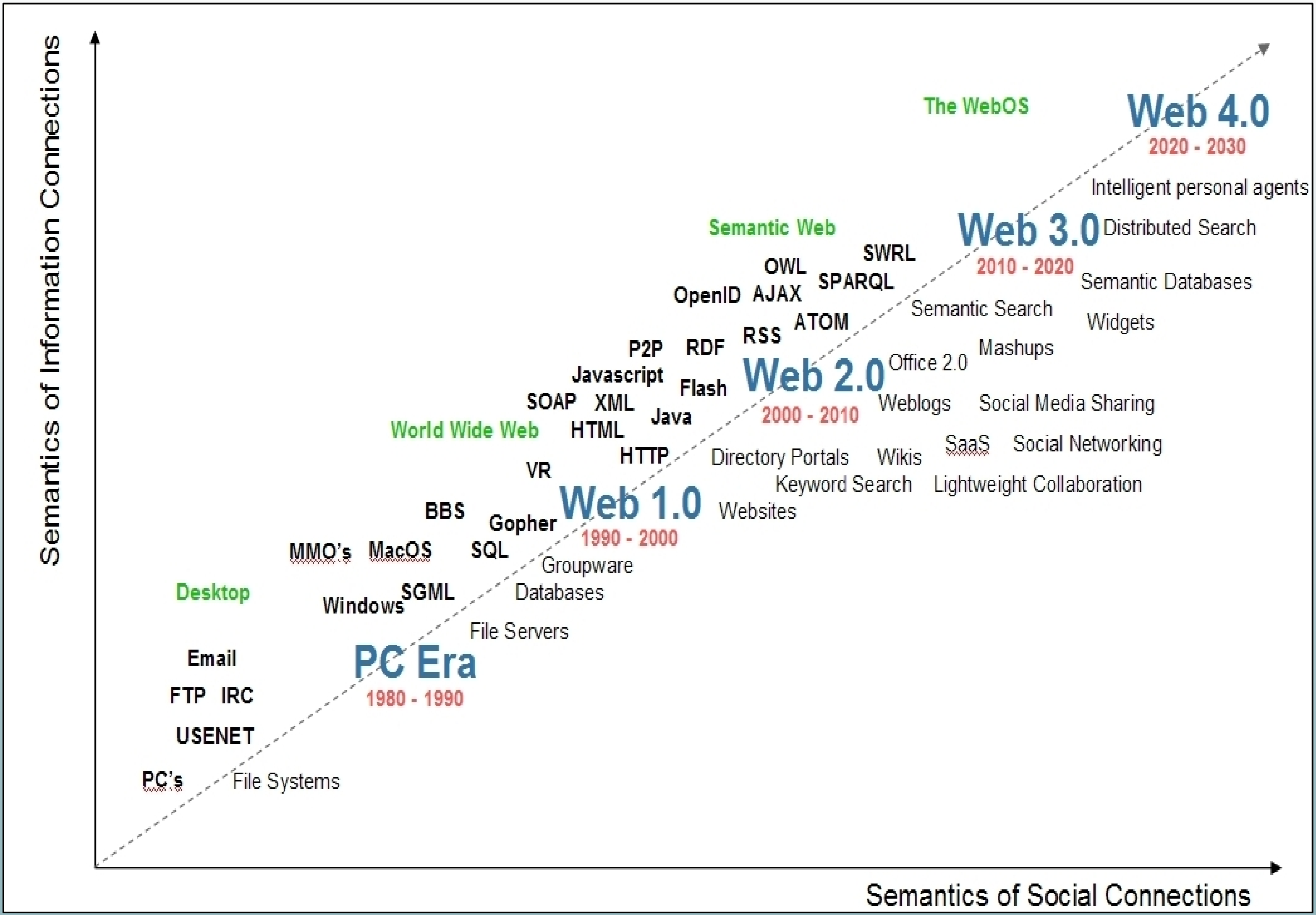
- Cavoukian, “Privacy by Design” (January 2009) www.ipc.on.ca/images/Resources/privacybydesign.pdf
- Cavoukian, Privacy by Design Foundational Principles (Aug 2009) www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf
- Privacy by Design Challenge (2009-) www.privacybydesign.ca

# Privacy by Design Foundations


By Default
Proactive / Preventative
Embedded
Respect For Users
End to End Lifecycle Protection
Visibility / Transparency
Positive Sum Full Functionality
Information Technology
Accountable Business Practices
Physical Design & Infrastructure

www.privacybydesign.ca

# From PC to Web 4.0



Radar Networks & Nova Spivack, 2007 – www.radarnetworks.com

# Evolution of Information Management

- **Web 2.0, Software as a Service (SaaS), Web Services, “cloud computing,” and the Grid**

  Each of these terms describes part of a fundamental shift in how data are managed and processed. Rather than running software on a desktop computer or server, Internet users are now able to use the “cloud” – a networked collection of servers, storage systems, and devices – to combine software, data, and computing power scattered in multiple locations across the network.

# Context: Web 2.0 and Beyond

- 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
- **Web 4.0?** – Ambient intelligence

# Cloud Privacy Concerns

- Jurisdiction
- Security
- Creation of new datastreams
- Function creep / misuse
- Lawful access
- Loss of ownership
- Lack of consumer control

**Reaching for the Cloud(s): Privacy Issues related to Cloud Computing**
*Office of the Privacy Commissioner of Canada* (March 2010)
www.priv.gc.ca/information/pub/cc_201003_e.cfm

# Overcoming Cloud Concerns

## Europe

- European Leaders’ Call for Global Data Protection Law to Overcome Cloud Security Weaknesses (Mar 2010)
- ENISA report: *Cloud Computing: Benefits, Risks and Recommendations for Information Security* (Nov 2009)
- RISEPTIS, ICT Trust and Security Research, EDPS (Feb 2010)
  - **Digital Life and Trust,**
  - **Trustworthy networking and computing services,**
  - **Management of Digital Identities in the Common European Framework,**
  - **Development of the Legal Framework of the EU with regard to the Protection of Data and Privacy**

## U.S.

- U.S. Policy makers, businesses debate role of Washington in cloud computing (Mar 2010)
- Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1* (Dec 2009)
- Coalition Pushes Rewrite of Online Privacy Law (Mar 2010)
  “Under current law, Internet users enjoy more privacy rights if they store data locally, a legal twist that some companies fear could slow the shift to cloud-based services unless it’s changed.”

# Identity and Privacy Crisis

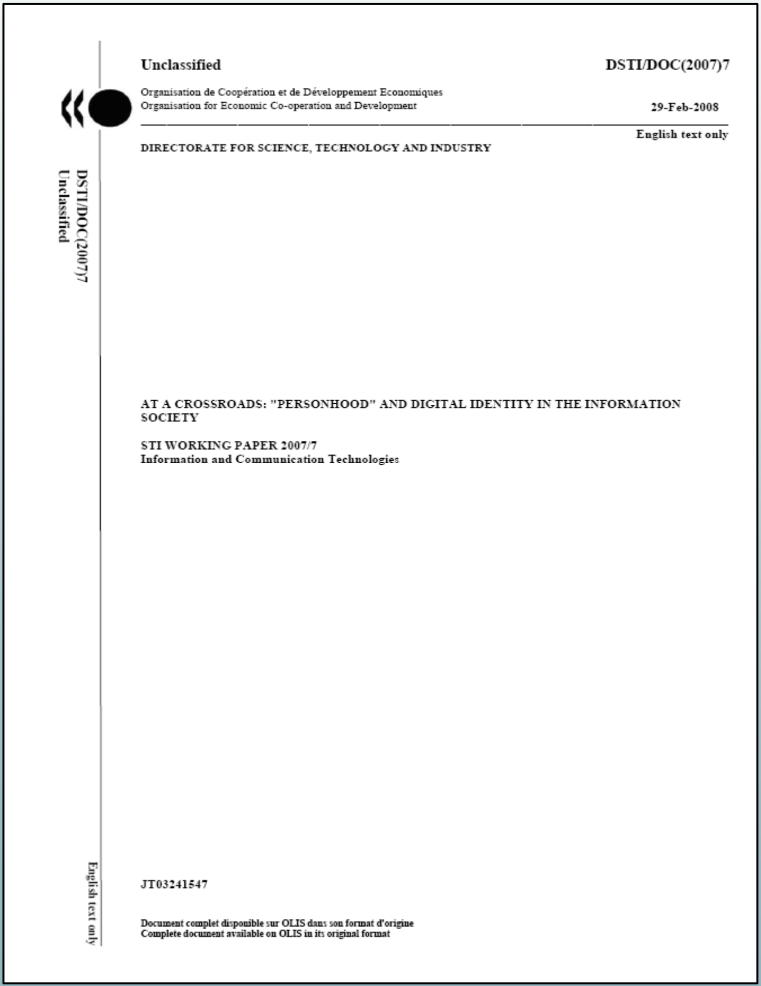
Growing ID requirements pose privacy problems:

- **Fraud and security concerns** are inhibiting confidence, trust, and the growth of e-commerce, e-government
- **Fears of surveillance** and excessive collection, use and disclosure of identity information by others are also diminishing confidence and use
- **Lack of individual user empowerment and control** over one's own personal data is diminishing confidence and use
- **Function creep, power asymmetries, discrimination, *harm***

**Needed:** improved user control, data minimization techniques, architectures of privacy, stronger security, trusted devices *and credible assurances*.

# *At a Crossroads: “Personhood” and Digital Identity in the Information Society*

1. Data Protection in the IDM-Enabled Ubiquitous Information Environment
2. Data Protection and User Control
3. Market Demand for User Control
4. The Properties of Identity
5. The Properties of Identity and Data Protection
6. The Properties of Identity for Policy Makers and Software Developers
7. Current Conceptions of IDM
8. Decisions and Constraints



**Unclassified** **DSTI/DOC(2007)7**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

**29-Feb-2008**

**English text only**

**DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY**

DSTI/DOC(2007)7
Unclassified

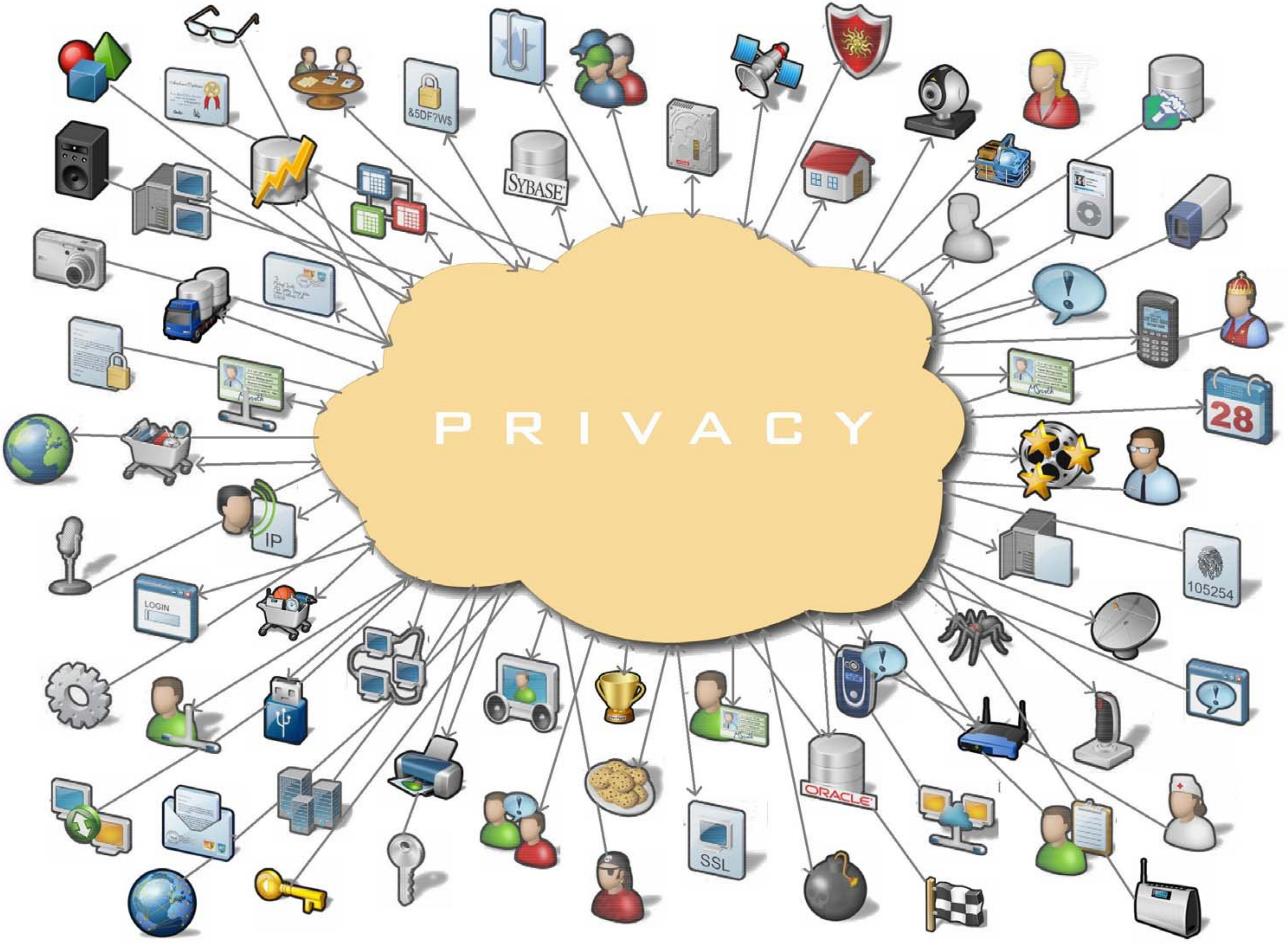
**AT A CROSSROADS: "PERSONHOOD" AND DIGITAL IDENTITY IN THE INFORMATION SOCIETY**

**STI WORKING PAPER 2007/7**
**Information and Communication Technologies**

English text only

**JT03241547**

**Document complet disponible sur OLIS dans son format d'origine**
**Complete document available on OLIS in its original format**


PRIVACY
&5DF?W$
SYBASE
IP
LOGIN
28
105254
SSL
ORACLE

# Privacy-Embedded

# Laws of Identity

# Building User-Centric Privacy into an Identity Metasystem

- Emergence of Identity Metasystem a profound development – strategic time to ensure that privacy interests are built into the new global architecture of identity
- Supporters of 7 Laws of Identity and Identity Metasystem call this the “Identity Big Bang” to enable ubiquitous intelligent services and a true marketplace 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

# "Privacy-Embedded" 7 Laws of Identity

1. **Personal Control and Consent:**

   *Technical identity systems must only reveal information identifying a user with the user's consent*

2. **Minimal Disclosure For Limited Use: Data Minimization**

   *The Identity Metasystem must disclose the least identifying information possible. This is the most stable, long-term solution. It is also the most privacy protective solution*

3. **Justifiable Parties: "Need To Know" Access**

   *Identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship*

# "Privacy-Embedded" 7 Laws of Identity

4. **Directed Identity: Protection and Accountability**
   *A universal Identity Metasystem must be capable of supporting a range of identifiers with varying degrees of observability and privacy*

5. **Pluralism of Operators and Technologies: Minimizing Surveillance** *The interoperability of different identity technologies and their providers must be enabled by a universal Identity Metasystem*

6. **The Human Face: Understanding Is Key**
   *Users must figure prominently in any system, integrated through clear human-machine communications, offering strong protection against identity attacks*

7. **Consistent Experience Across Contexts: Enhanced User Control**
   *The unifying Identity Metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies*

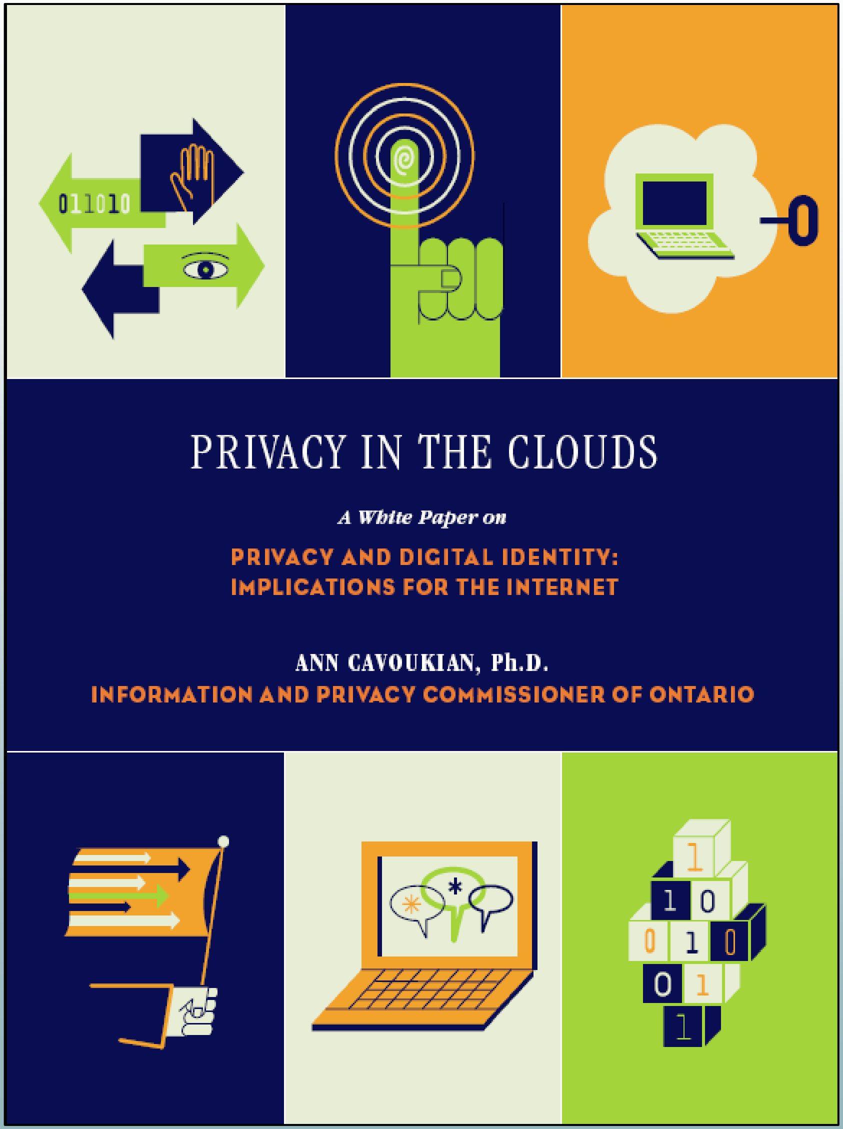
# Implications for Users

**The 7 Privacy-Embedded "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 web sites (less spam, phishing, pharming, online fraud).

# Privacy in the Clouds

- The 21st Century Privacy Challenge
- Creating a User-Centric Identity Management Infrastructure
- Technology Building Blocks
- Call to Action



PRIVACY IN THE CLOUDS

*A White Paper on*

PRIVACY AND DIGITAL IDENTITY:
IMPLICATIONS FOR THE INTERNET

ANN CAVOUKIAN, Ph.D.
INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

www.ipc.on.ca/images/Resources%5Cprivacyintheclouds.pdf

# The 21$^{st}$ Century Privacy Challenge

## Power and Promise of Cloud Computing:

- Limitless flexibility
- Better reliability and security
- Enhanced collaboration
- Portability
- Simpler devices

# The 21st Century Privacy Challenge

**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
- Are transparent and lend themselves to audit

# Creating A User-Centric Identity Management Infrastructure

- Adequate tools to manage personal information on all devices
- Infrastructure allowing unified user experience with all devices
- System with a clear framework of agreed upon rules
- “Sticky” policies that travel with the information and ensure proper use in accordance with policy
- Infrastructure that supports cross-system interaction as well as interoperation and delegation
- Open standards and community-driven interoperability
- Policies, mechanisms, and technologies that use only the amount of personal information necessary
- Diversity in identity management systems

# Cloud Technology Building Blocks

- Open source and proprietary identity software based on open standards
- Federated identity
- Multiple and partial identities
- Data-centred policies
- Audit tools

# A Call to Action

- Corporate and individual users can explore the evolving identity systems and demand that they have privacy protection built in, as well as implementing open standards so that different systems will be truly interoperable;
- Standards bodies can continue to develop and promote the fundamental standards needed for identity systems, data-centered poli-cies, and privacy-enhancing technologies;
- Software vendors and website developers can embrace privacy-enhancing technologies, open standards, open identity management systems, and true interoperability;
- Governments, through their procurement decisions, can support the development of open identity management systems that are designed to meet user needs for privacy, interoperability, and flexibility.

# Federated Privacy Impact Assessment (F-PIA)

## Goals of an F-PIA:

- Provide an opportunity for members to develop and codify a Federation’s privacy policies;
- Demonstrate that privacy policies, as defined by members of the Federation, will be met;
- Demonstrate that an appropriate technological architecture is in place to prevent, to the extent possible, accidental or malicious violations of privacy policies.

The New
Federated Privacy Impact Assessment
(F-PIA)

Building Privacy and Trust-enabled
Federation

Information and Privacy
Commissioner of Ontario

Liberty Alliance Project

January 2009

# Four Fundamental Approaches

1. Trust the data to behave
2. Trust personal devices to interface and act on our behalf
3. Trust intelligent software agents to behave
4. Trust intermediary identity providers to behave

# Through the Clouds

**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.

# Questions? Comments?

???

# How to Contact Us

## Ken Anderson

**Office of the Information & Privacy Commissioner of Ontario**

**2 Bloor Street East, Suite 1400**
**Toronto, Ontario, Canada**
**M4W 1A8**

| | |
|---|---|
| **Phone:** | **(416) 326-3333 / 1-800-387-0073** |
| **Web:** | **www.ipc.on.ca** |
| **E-mail:** | **info@ipc.on.ca** |