Clouds, Crowds & Government Shrouds

Ken Anderson
Assistant Commissioner (Privacy)
Ontario

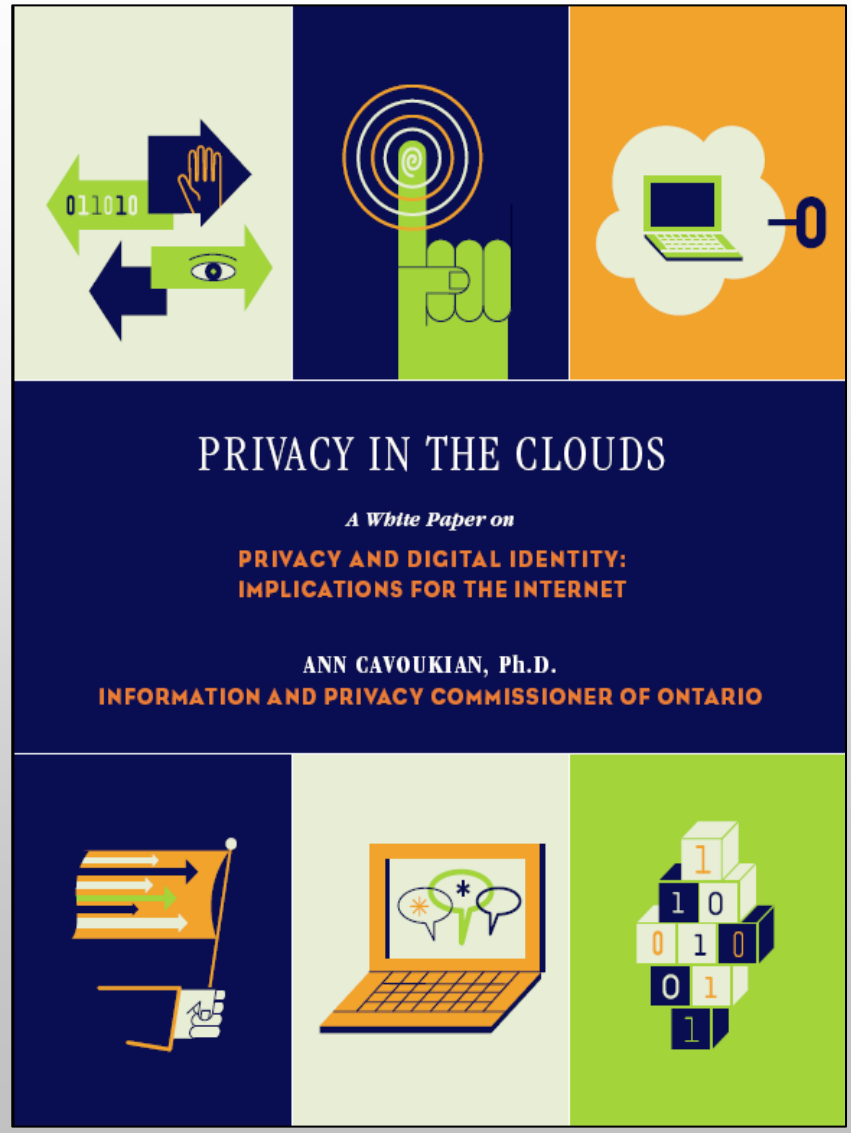
Access and Privacy Conference 2008
Edmonton, Alberta
June 20, 2008

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*

Privacy in the Clouds

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



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

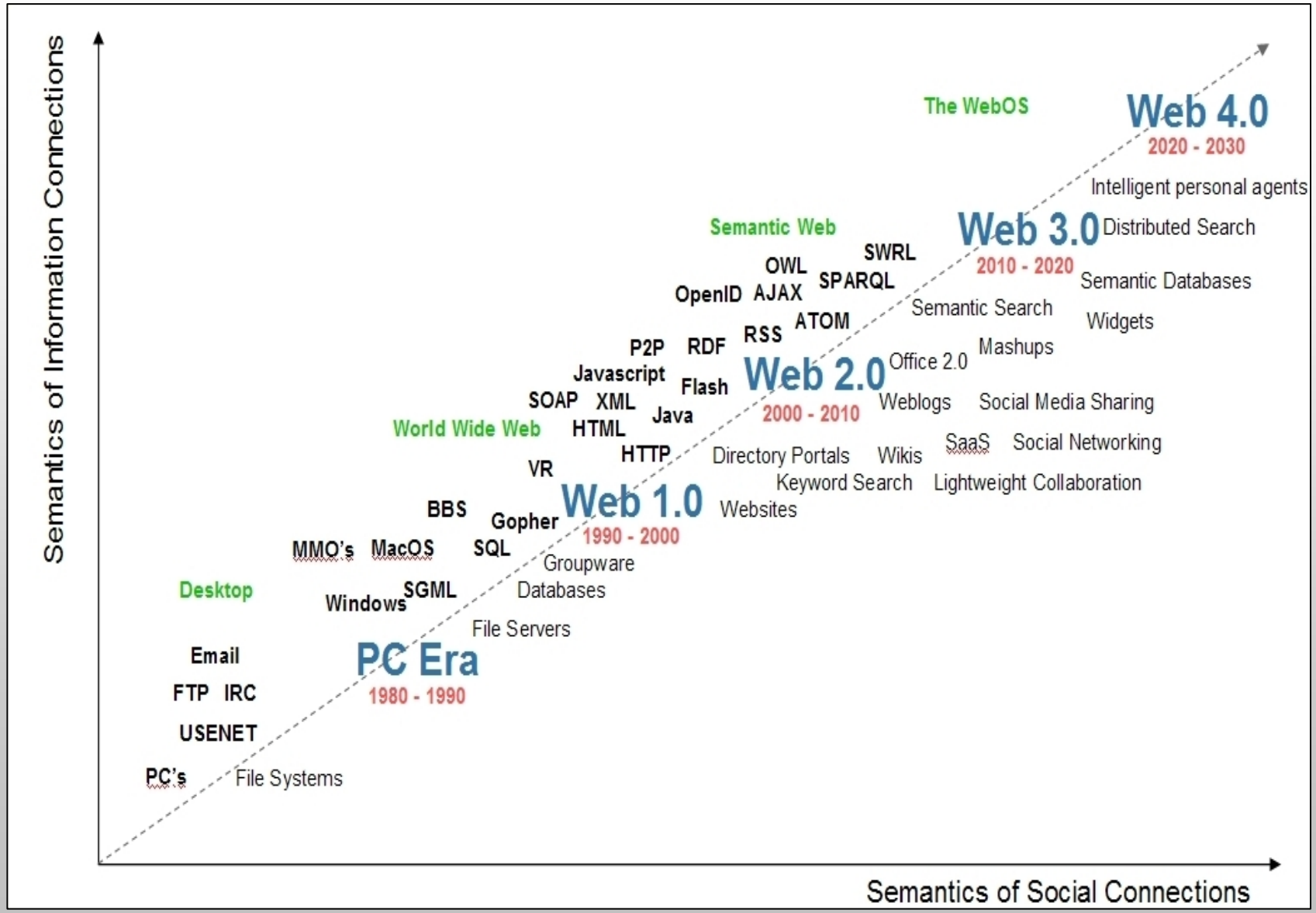
Context:
Web 2.0 and Beyond

- 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.

From PC to Web 4.0



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

Why Privacy is an Issue in Web 2.0 , 3.0 and 4.0

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

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;

- **Personal information**, be it biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational or reputational, is the stuff that makes up our modern identity. It must be managed responsibly. When it is not, accountability is undermined and confidence in our evolving information society is eroded.

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.

Problem

On the Internet, users usually have to establish their identity each time they use a new Internet-based application, usually by filling out an online form and providing sensitive personal information (e.g., name, home address, credit card number, phone number, etc.).

This leaves a trail of personal information that, if not properly protected, may be exploited and abused.

Identity Service Requirements in the Cloud

Cloud computing requires identity services that:

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

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.

Case Studies

1. The “Live Web”
2. Online Dating
3. Cell Phone Payments and Location-Dependent
4. Services
5. Health Care Records
6. Identity and Trust in Virtual Worlds

Creating A User-Centric Identity Management Infrastructure

- Adequate tools to manage personal information on all devices;
- Infrastructure that allows 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;
- A great deal of diversity in identity management systems.

Cloud Technology Building Blocks

1. **Open source and proprietary identity software based on open standards;**
2. **Federated identity;**
3. **Multiple and partial identities;**
4. **Data-centred policies;**
5. **Audit tools;**

Cloud Technology Building Blocks
Open Source

Open source and proprietary identity software based on open standards which can be easily incorporated into the full range of online services and devices (similar to the open source software that is at the core of the Internet and the Web today).

Cloud Technology Building Blocks
Federated Identity

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.

Cloud Technology Building Blocks
Multiple and Partial Identities

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

Cloud Technology Building Blocks
Data-Centered Policies

Data-centered policies that are generated when a user provides personal or sensitive information, that travels with that information throughout its lifetime to ensure that the information is used only in accordance with the policy, e.g., for the purposes for which it was intended which the user had consented to.

Cloud Technology Building Blocks
Audit Tools

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

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 funda-mental 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 manage-ment 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.

Four Fundamental Approaches

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

Four Fundamental Approaches

1. **Trust the data to behave:** New privacy-enhancing information technologies make it possible to attach individual privacy rights, conditions and preferences directly to their own identity data, similar to digital rights management technologies;

2. **Trust the personal device to interface and act on our behalf:** The many technologies that travel with us are growing in storage, computing, and communications sophistication. Cell phones, PDAs, “smart” cards and other tokens under our physical control are becoming our de facto digital wallets, interacting with the “grid” and serving as brokers for our identity-based transactions in the digital worlds. These devices need to be trustworthy, fully user-configurable, user-transparent and easy to use.

Four Fundamental Approaches

3. **Trust the intelligent software agents to behave:** Whether operating on our "always-on" internet devices, or housed somewhere in the Cloud, intelligent software agents can automatically and continuously scan, negotiate, do our bidding, reveal identity information, and act on our behalf in a Web 2.0 world. Some examples may include delegated identity tools, "reachability" software, and "privacy bots;"

4. **Trust intermediary identity providers to behave:** Inevitably, we must also have sufficient trust in those organizations that would supply and accept our identity credentials and our personally identifiable information. In a federated identity world, these trusted actors will increasingly act on our behalf, disclosing our identity data for the purposes we define in advance, and under specific conditions. They must find credible technological mechanisms for assuring us that they are behaving in an open and accountable manner, and that our privacy is in fact being protected.

IPC Involvement

- **7 Privacy-Embedded Laws of Identity**
- **Federated Privacy Impact Assessment**
- **Sticky Policies**

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

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