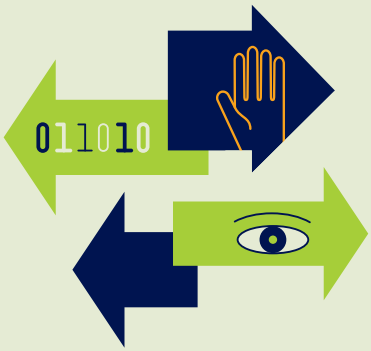
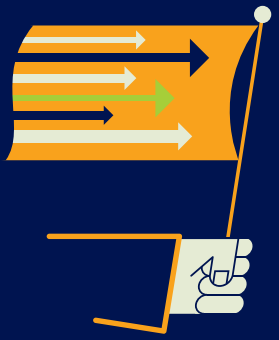


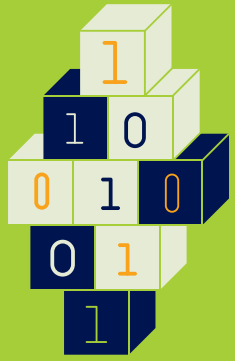
PRIVACY IN THE CLOUDS

A White Paper on

PRIVACY AND DIGITAL IDENTITY: IMPLICATIONS FOR THE INTERNET

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





PRIVACY IN THE CLOUDS

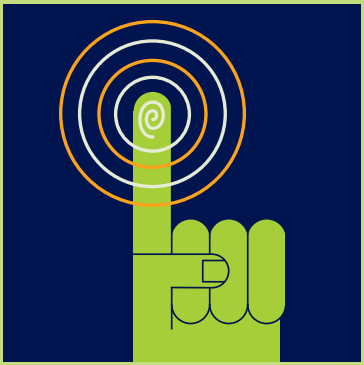
A White Paper on

PRIVACY AND DIGITAL IDENTITY: IMPLICATIONS FOR THE INTERNET

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

TABLE OF CONTENTS

The IPC would like to acknowledge and sincerely thank IBM Research Systems & Software experts, in particular, Dr. Jan Camenisch, Anthony Nadalin, Michael R. Nelson and Dr. Michael Waidner, for their contributions.



INTRODUCTION

Informational self-determination refers to the ability of individuals to exercise personal control over the collection, use and disclosure of their personal information by others. It forms the basis of modern privacy laws and practices around the world.

All organizations that collect and use personal data must accommodate the legitimate interests of individuals. Organizations can do this, for example, by being open and accountable about their information management practices, by seeking informed consent, and by providing individuals with access and redress mechanisms. At stake is not only privacy, but the confidence and trust of millions of individuals, consumers, and citizens in today's information society.

At the Office of the Information and Privacy Commissioner of Ontario (IPC), we have long advocated a strong role for individuals in managing their personal information, not just by exercising their privacy rights under Ontario law, but also by becoming better informed and using privacy-enhancing technologies (PETs). PETs can minimize the disclosure and (mis)use of personally-identifiable information (PII), and help secure data from unauthorized use by others.

Informational self-determination has become a challenging concept to promote and protect in a world of unlimited information passing from individuals to organizations, and from organizations to each other, often described as 'Web 2.0'. As a result of widespread developments in information and communications technologies (ICTs), we are collectively creating, storing and communicating information at nearly exponential rates of growth. A large majority of this data is personally identifiable, and much of it is under the control of third parties. Practical obscurity – the basis for privacy norms throughout history – is fast disappearing.

Our digital footprints and shadows are being gathered together, bit by bit, megabyte by megabyte, terabyte by terabyte, into personas and profiles and avatars – virtual representations of us, in a hundred thousand simultaneous locations. These are used to provide us with extraordinary new services, new conveniences, new efficiencies, and benefits undreamt of by our parents and grandparents. At the same time, novel risks and threats are emerging from this digital cornucopia. Identity fraud and theft are the diseases of the Information Age, along with new forms of discrimination and social engineering made possible by the surfeit of data.

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.

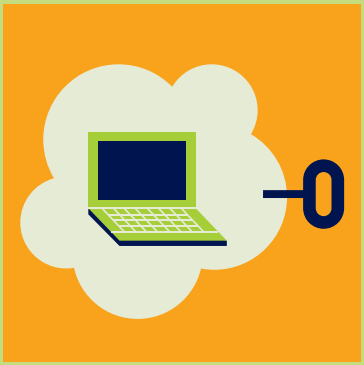
It may very well be that our fundamental ideas about identity and privacy, the strategies that we have collectively pursued, and the technologies that we have adopted, must change and adapt in a rapidly evolving world of connectivity, networking, participation, sharing, and collaboration.

What will privacy mean, and how will privacy survive and hopefully thrive, as a viable human right, operational value, and critical enabling trust factor in a world where the individual is less and less directly present in the midst of data-rich transactions?

How will individuals exercise control over their personal data when that data is stored and processed in the Cloud[1] – that is, everywhere except on their own personal computing devices?

Profound and dramatic transformations and upheavals are on the way. How will privacy fare?

[1] In telecommunications, a "cloud" is the unpredictable part of any network through which data passes between two end points. For the purposes of this paper, the term is used to refer generally to any computer, network or system through which personal information is transmitted, processed and stored, and over which individuals have little direct knowledge, involvement, or control.



THE 21ST CENTURY PRIVACY CHALLENGE

The Internet has entered into a new phase. Thanks to more reliable, affordable, and ubiquitous broadband access, the Internet is no longer just a communications network. It is becoming a platform for computing – a vast, interconnected, virtual supercomputer. Many different terms have been used to describe this trend: 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.

The importance of this shift cannot be overstated. To quote Nicholas G. Carr, it "will overturn strategic and operating assumptions, alter industrial economics, upset markets and pose daunting challenges to every user and vendor. The history of the commercial application of information technology has been characterized by astounding leaps, but nothing that has come before – not even the introduction of the personal computer or the opening of the Internet – will match the upheaval that lies just over the horizon."[2]

[2] Nicholas G. Carr, The End of Corporate Computing, MIT Sloan Management Review, Spring 2005, pp. 67-73

The new digital ecosystem will also present complex security and privacy challenges. Fundamentally, it will need to provide flexible, user-friendly ways to authenticate users. Without better management of digital identities, we will not only continue to struggle with existing problems such as identity theft, spam, malware, and cyber-fraud, we will be unable to assure individual users that they can safely migrate their critical data and applications from their own computers onto the Web. The opportunity presented by technological development will be lost.

EVOLUTION OF CONSUMER COMPUTING

From a user's perspective, the evolution of consumer computing can be divided into three phases:

1. **The stand-alone personal computer** in which the user's operating system, word processing system, database software and data are stored on a single, easily protected machine. Examples: word processing, spreadsheets on a stand-alone server.
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. Example: using a Web browser to read a Web page.
3. **The "Cloud"**[3] in which users rely heavily on data and software that reside on the Internet. Examples: using Amazon's Simple Storage Service (S_3) and Elastic Computing Cloud (EC_2) to store unlimited photos on Smugmug, an online photo service; using Google Apps for Word-processing; virtual worlds such as Second Life that enable users to build 3-D environments combining Web pages and Web applications (e.g. feeding a Webcast into a virtual theatre); grid computing.

[3] See "The Information Factories" by George Gilder, Wired magazine, October, 2006, http://www.wired.com/wired/archive/14.10/cloudware_pr.html

THE POWER AND PROMISE OF CLOUD COMPUTING

Most of the work we do with computers is still conducted using phase 1 or 2 tools, but more and more people – especially younger generations – are starting to take advantage of the power of the Cloud. The Cloud offers them so much:

1. **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, share their ideas, and enjoy online games, video, and virtual worlds;
2. **Better reliability and security:** Users no longer have to worry about their hard drives crashing or their laptops being stolen;
3. **Enhanced collaboration:** By enabling online sharing of information and applications, the Cloud offers users new ways of working and playing together;
4. **Portability:** Users can access their data and tools wherever they can connect to the Internet;
5. **Simpler devices:** With data and the software being stored in the Cloud, users don't 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 built into their clothing.

We can only enjoy the full benefits of Cloud computing if we can address the very real privacy and security concerns that come along with storing sensitive personal information in databases and software scattered around the Internet.

Digital identity is a fundamental challenge. In phase 1 of consumer computing, users' privacy and security was largely assured by restricting physical access to the stand-alone computing devices and storage media. Identity needs were fairly minimal, consisting largely of a small handful of usernames and passwords for local systems and file access.

In phase 2 of consumer computing, 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 and the exciting tools it makes possible (like virtual worlds, grid computing, and shared archives), require identity services that:

1. are independent of devices;
2. enable a single sign-on to thousands of different online services;
3. allow pseudonyms and multiple discrete (but valid) identities to protect user privacy;
4. are interoperable, based on open standards, and available in open source software (in order to maximize user choice);
5. enable federated identity management; and
6. are transparent and auditable.

This paper explores what will be possible if proper digital identity services are deployed and the full power of Cloud computing is realized. A number of scenarios are described:

1. an identity service that enables individuals to easily manage their own online identities and to effortlessly participate in online collaboration activities without repeated sign-ons;
2. an identity tool that gives users of an online dating service better privacy than is available from today's sites;
3. a payment system using cell phones or RFID chips that has privacy built in;

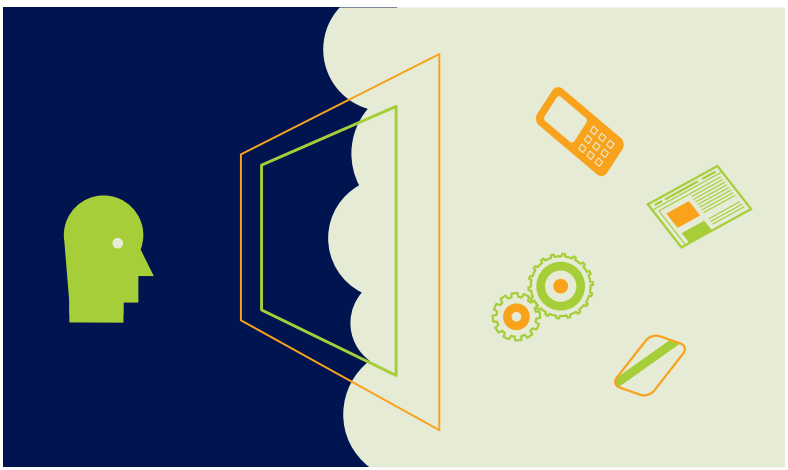
4 an infrastructure for electronic health records; and

5 an identity service for virtual worlds such as Second Life.

THE DIGITAL IDENTITY SITUATION 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 identity information to be given from one party to another. Today, most users have to establish their identity each time they use a new application, usually by filling out an online form and providing sensitive personal information (e.g., name, address, credit card number, phone number, etc.).

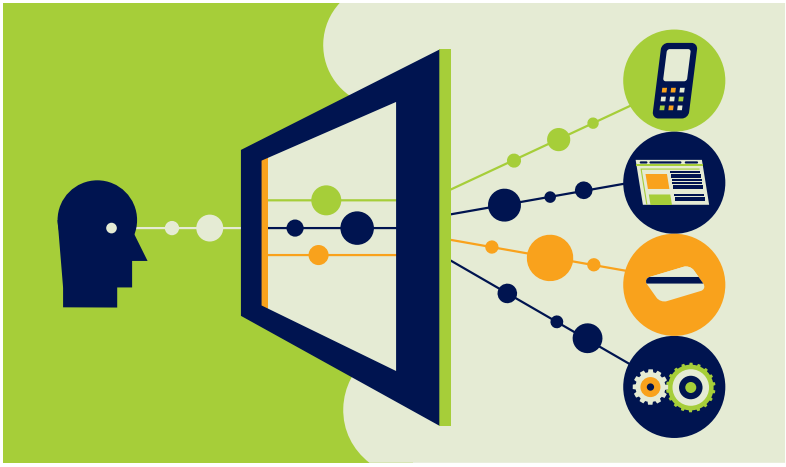
A typical Internet user in Canada has provided some type of personal information to dozens of different websites. If you count cookies and IP addresses as personal information, then Internet users have left behind personally identifiable information everywhere they've been. They have left "digital bread crumbs" throughout cyberspace – and they have little idea how that data might be used or how well it is protected.



THE DIGITAL IDENTITY NEEDS OF TOMORROW

What is needed is flexible and user-centric identity management. Flexible because it needs 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. Users must be empowered to execute effective controls over their personal information.

In the future, users will not have to re-enter personal data each time that they go to a new website. Instead, by using an identity service (or two or more different ones), they will have control over who has their personal data and how it is used – minimizing the risk of identity theft and fraud. Their identity and reputation will be transferable. If they establish a good reputation, for example, at an auction site, they will be able to use that fact on other sites as well. One result of this would be greater choice of online services, since users would not be locked into one service or vendor.



A truly flexible identity management system would not be limited to laptop and desktop computers; it would work on cell phones, personal digital assistants, smart cards, sensors, consumer electronics like video recorders and online game consoles – any way that a user might touch the Internet. This approach to digital identity will unleash the full potential of the Cloud, enabling users to seamlessly tap into and combine a wide range of online services.

CASE STUDIES

1 THE "LIVE WEB"

The Internet has become a vastly more connected and interactive place for millions of people to spend their time. By any measurement index – growth in 'blogs, collaborative wikis, mash-ups, and online social networks – the phenomenon of the "participatory Web" is transforming our lives with virtually limitless opportunities to become engaged, customize experiences, and find our own individual public voices.

This proliferation of online activity requires sound identity management. With the increased use of the Internet to conduct business and the rise of new types of online interactions, such as social networking and user-generated content, innovative kinds of digital identifier technologies are necessary to sustain the "open Web." Online users need to securely manage their multiple accounts and passwords across multiple domains, without fear of surveillance and profiling.

In order to facilitate this, OpenID, developed by an open community, is free "user-centric" digital identity technology that simplifies the online user experience by reducing the complexity of managing dozens, even hundreds of

user names and passwords across Internet sites, and providing greater control over the personal information users are required to share with websites when they sign in.

OpenID enables individuals to convert one of their already existing digital identifiers – such as their personal blog's URL – into an OpenID account, which can then be used as a log-in at any website supporting OpenID.

Today, more than 10,000 websites support OpenID log-ins, and an estimated 350 million OpenID-enabled URLs currently exist.

For online businesses, these efforts can lower password and account management costs, help reduce the overall risks of security breaches by limiting the amount of customer personal information they need to store and protect, and increase both new and return user traffic by lowering the barriers to website entry and re-entry.

2 ONLINE DATING

An online dating service matches people together based on their personal interests and preferences using some sophisticated matching algorithms. The matching algorithm needs a good deal of personal data in order to work, and therefore users of those dating services need strong assurances that their information will be treated with respect and used only for the intended and agreed-upon purposes.

Even if a user agrees to receive marketing emails from third parties, for example, they may nonetheless want to be certain that their personal details will not be given to those third parties. For instance, someone who is overweight may not wish to receive marketing e-mails from makers of "full-size" clothing.

To protect privacy, dating services could allow their clients to use pseudonyms rather than their real names. The dating service has no business need to know

the real identities of their customers, other than their need to get paid, which could be done through a pre-paid or cash-like service.

Today, customers of dating services can claim almost any attribute, and nothing prevents "devils" from impersonating "angels." With better digital identity management, the dating service would be able to accept third-party certified attributes, without customers running the risk that the certificates would reveal their real names to the service. For instance, a certified date of birth might give a higher rank in the matchmaking algorithms than an uncertified one. A certificate that a customer is not listed in a certain blacklist might be mandatory for certain dating services. Such an approach would reduce the risk of misrepresentation and increase the level of trust, without impacting on privacy.

When customers finally get introduced to each other, they could potentially use the identity management mechanisms to establish increasing trust in each other in a multi-round "game," checking each others' attributes in the safety and privacy of their homes. They could even ask each other questions like "are you younger than me?" and so on, without having to reveal their actual birthdays, but rather, just a birth year or range.

3 CELL PHONE PAYMENTS AND LOCATION-DEPENDENT SERVICES

One very promising development in the cell phone industry is the deployment of cell phones as "digital wallets" that can be used to transfer and store money, pay parking meters and vending machines, and eventually act as a kind of a credit card. Privacy concerns, however, are a major barrier to the adoption of this technology.

Many consumers are already uncomfortable knowing that credit card companies can compile a detailed record of their spending behavior. With electronic

wallets, it is conceivable that your cellular phone provider would not only know when, where, and how you were spending your money, but by tracking others' electronic wallets, they could know who you were with when you spent it (at a restaurant or a hotel, for instance).

User-centric identity management would allow the users of an "electronic wallet" to use a digital identity service to authenticate themselves, without revealing their actual identity to either vendors or network providers.

4 HEALTH CARE RECORDS

Some of the most sensitive personal information about us is associated with the medical services and medications we use. Yet today, that personal information is scattered in dozens of different locations including doctors' offices, pharmacies, insurance companies, and our places of employment.

One of the biggest barriers to the widespread adoption of electronic health records has been the concern of patients that their data in such records will be misused or stolen. We have already seen too many examples of sensitive medical or drug data being used for inappropriate or unauthorized purposes.

User-centric identity management could ensure that someone's real name (and the personal data that could be used to infer who they are) would be protected and kept separate from the details of their medical records, insurance claims, and drug prescriptions. It would also enable a patient to use an online portal with a federated identity system to quickly and safely access all their medical information, whether it be stored at their doctor's office, their pharmacy, or their insurance company. Perhaps most importantly, there would be the ability to audit these records and determine where personal data is stored, how it is protected, and who has had access to it.

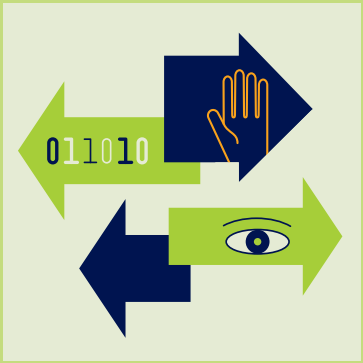
5 IDENTITY AND TRUST IN VIRTUAL WORLDS

Over the last year, there have been a number of press reports on virtual worlds such as Second Life and There.com, and online games such as World of Warcraft. Millions of people are spending hours a week in these immersive, three-dimensional online environments, finding new ways to collaborate, play games, and share information. Virtual economies are also developing as inhabitants of these virtual worlds buy and sell virtual goods and services, exchanging millions of real dollars every year.

Unfortunately, there are currently no effective means for managing identity and security in most virtual worlds. As a result, it is difficult to prevent disruptive behavior or inappropriate postings by anonymous users who may appear and quickly disappear. This lack of security and trust is slowing the development of serious business applications in virtual worlds.

User-centric identity management could provide an effective way to build trusted communities in the virtual world. For instance, parents could rest assured that when their children went online to play in a virtual world for kids, every other person there had been properly authenticated and was really a "child."

One of the most exciting reasons for the phenomenal growth of virtual worlds like Second Life is that they allow users to create new services and to "plug in" applications from elsewhere on the Web. With user-centric identity management, you could establish your identity once and then be able to use the full range of services in a virtual world. And an identity established in Second Life could then be transferable into another virtual world. But you would not have to share your personal information in any other "world" unless you chose to.



CREATING A USER-CENTRIC IDENTITY MANAGEMENT INFRASTRUCTURE

The goal of a flexible, user-centric identity management infrastructure must be to allow the user to quickly determine what information will be revealed to which parties and for what purposes, how trustworthy those parties are and how they will handle the information, and what the consequences of sharing their information will be. In other words, these tools should enable users to give informed consent. The default should be minimal disclosure, for a defined purpose. Any secondary or additional use should be optional after enrolment.

Companies need to understand that identity management is not only a business process, but also a user activity. Users must be given adequate tools to manage the personal information on all of their devices. This means that the identity infrastructure must account for many devices, from desktop PCs to mobile phones. The infrastructure must allow for a unified user experience over all devices.

It also means that the system must be driven throughout by a clear framework of agreed-upon rules. This includes policies describing to users what information is requested and why (similar to a machine-readable and improved version

of today's privacy policies). It must also include a "sticky" policy that travels with the information throughout its lifetime and ensures that it is only used in accordance with the policy. The last step will of course require mechanisms to enforce these sticky policies in ways that can be verified and audited.

There are already a number of identity management systems in place on a wide variety of platforms. These need to be supported, at least in the short term, by the identity management infrastructure. The infrastructure must support cross-system interaction as well as interoperation and delegation between them. This is only possible if the infrastructure and the individual systems are based on open standards, available on all platforms. For a successful user-centric identity management infrastructure to emerge, it is crucial that its development be driven by a wide and open community, spanning over the different geographies and cultures, and that open source implementations of all of its infrastructural components be made available.

Identity information is almost always personally identifiable information, which is governed by special privacy regulations in many parts of the world. Further, an improper use of identity information may lead to identity theft and other breaches of security. Thus, identity information requires special protection. This includes, among other things, the ability to carry and enforce sticky policies, encrypt data, and minimize the amount of identity information used by various applications. Actual identity management systems will support a wide variety of privacy and various security properties, ranging from low-security password-based one-factor authentication to high-end, attribute-based systems deploying state-of-the-art privacy-enhancing certificates (for example, IBM's Identity Mixer technology, or Microsoft's U-Prove technology.). While the infrastructure needs to support all of these systems, users should understand the implications of using one system over the other.

At the end of the day, applications need to be able to make use of the infrastructure. This requires that applications be presented with a unified view and interfaced to this infrastructure across different platforms and devices. These interfaces should be independent of the actual protocols and mechanisms that are used to convey the identity information underneath. Therefore, we are proposing a single architecture that pulls the different pieces together and unifies them.

By supporting a plethora of identity systems, this architecture will allow for the migration of applications from legacy systems to the user-centric ones that will emerge and prevail. To enable such migration, as well as building applications from scratch, adequate tools and sample applications will need to be provided.

OPEN STANDARDS AND COMMUNITY-DRIVEN INTEROPERABILITY

The Internet was founded on open standards and collaboration. Open standards facilitate a reliable base for customers, applications, and enterprises. As such, they form an important foundation for the growth of the future Web and nurture the development of an open identity management ecosystem for the whole industry.

To enable the federation and interoperability of the different existing and emerging identity management systems, the underlying standards and specifications need to be complete, freely accessible, and, most important, driven by the community. To have user-centric identity management widely adopted, the standards and tools provided need to be free from IP infringements. This will allow for a supporting ecosystem to grow and be maintained, not only by multinational companies but also by open-source initiatives and start-ups. So it is essential that standards be published widely and on a timely basis, and that they be stable and enduring.

Open standards are required to support the plethora of environments and application scenarios in which identity management plays a critical role and to enable inter-operation of these environments. In particular, communication formats and policy specifications act as medium for the interconnection of client and server-sides. This medium can only form the basis for a lively and value-generating ecosystem if it is based on the principles of truly open standards.

The standards – rather than the particular implementations by single vendors or consortia – must form the basis of regular interoperability tests. Moreover, they need to be controlled by an impartial, credible standards organization that governs the freely available open standards for the benefit of the entire community.

PROTECTING PRIVACY

The Internet was designed to connect and authenticate devices with logical and physical address spaces. User-centric identity services can provide the same ubiquitous connectivity for individuals. An identity today is no longer a single number assigned to an individual but rather comprises a set of attributes including address, birthdate, degrees held, and personal preferences. Such personal information requires special protection, not only to prevent fraud and identity theft, but also to comply with privacy laws.

Most existing laws have their roots in the Organisation for Economic Co-operation and Development's (OECD) privacy guidelines. These stipulate, for example, that only the personal information needed for a stated purpose should be collected, that the collection should be openly communicated, that the user must give informed consent to the collection and use, and that the personal information must be properly safeguarded.[4]

[4] In 2006 the IPC led an international group of privacy and data protection commissioners to develop a set of fair information practices that harmonized the various privacy codes and practices currently in use around the world. The result – the Global Privacy Standard – can be found at: www.ipc.on.ca/images/Resources/up-gps.pdf

Identity management systems can support compliance with privacy laws through the use of privacy policies, enforcement mechanisms, and technologies that allow applications to use only the amount of personal information that is strictly necessary to the application. Policies that outline what information is being sought and the reasons why enable users to give informed consent. These policies will also govern access controls, and should travel with the data for the course of their lifetime.

Already there exist privacy-enhancing technologies that allow a user to give an authentication token containing only an encrypted form of the user's identity to a service provider. This allows the user to appear anonymously to the service provider while still making it possible to reveal true identity in the event of an investigation by a designated authority. Strong restrictions and conditions would be placed on an authority's ability to revoke a user's anonymity.

DIVERSITY FOR A LIVELY ECOSYSTEM

There is currently a great deal of diversity in identity management systems, along with a multitude of open standards that support identity federation and user-centricity for these systems. The most prominent examples are probably SAML, OpenID, and the WS-Federation specifications. Each of these has pros and cons, and contributes in different ways to the emerging ecosystem.

While these efforts will likely converge over time, the present diversity may be inspiring and potentially drive positive new developments in identity management. New models and protocols are being developed and deployed. Further methods will evolve, and there will be niches and application scenarios in which some specific solutions will surpass mainstream standards and protocols.

Investments have already been made in deploying system-based identity management products like Liberty Alliance or WS-Federation. The emerging

ecosystem needs to support the existing diversity while allowing new solutions and concepts to be applied, as other solutions fade out gracefully.

DIVERSITY FOR USER DEVICES

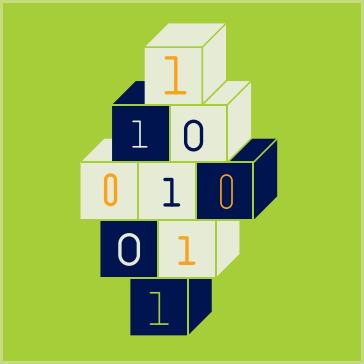
While user-centricity is mostly discussed with PCs in mind, users will want to use a number of other devices such as mobile phones or electronic identity cards to take part in the information society. They may even wish to use devices that they do not personally own.

This diversity of clients requires that the identity management system be flexible, offering users a maximum number of choices as well as the best security and privacy protection possible.

COLLABORATION OF USERS

The boundaries of corporations are becoming less defined, with virtual companies emerging. Further, user contributions and collaboration are becoming increasingly central to many emerging applications. These scenarios have in common the need to deal with users who have not been physically identified but are judged by their reputation or other attributes (such as area of expertise, education, age, etc.), as attested to by third parties.

The emerging identity information infrastructure must support such a collaborative environment – allowing for decentralized and federated trust models based on limited identity information (e.g., the current user is a medical expert).

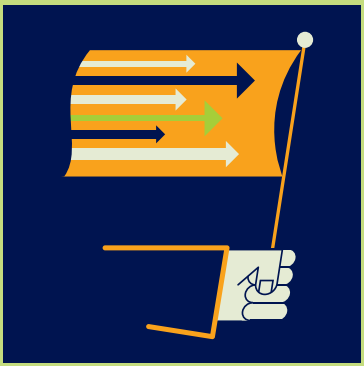


TECHNOLOGY BUILDING BLOCKS

These different scenarios will require a number of different technology building blocks, including:

- **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).
- **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.
- **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.

- **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.
- **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

It will not be possible to realize the full potential of the next generation of the Internet and Cloud Computing without developing better ways of establishing digital identity and protecting privacy.

Fortunately, progress is being made in developing and deploying the technological tools needed. But barriers remain. Different segments of the "IT ecosystem" can take steps to overcome them:

- 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 policies, 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.

The brave new world of Cloud Computing offers many benefits provided that the privacy and security risks are recognized and effectively minimized.

User-centric private identity management in the Cloud is possible, even when users are no longer in direct possession of their personal data, or no longer in direct contact with the organization(s) that do possess it.

This paper has outlined some technical building blocks and challenges that will become essential elements of a privacy-friendly Web 2.0 world. To be sure, laws, standards, education, awareness, and market forces will also be needed to support this vision.

Widespread and enduring user trust depends on realizing this vision. But how can we collectively assure confidence and trust in the privacy of our personally identifiable information, when our identity data is held by others and we are not directly involved in data transactions in Cloud?

Four fundamental technological approaches present themselves:

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 for intellectual property.

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 and proxies for our identity-based transactions in the digital worlds. These devices need to be trustworthy, fully user-configurable, user-transparent and easy to use.

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. Possible technologies might include automated audit and enforcement tools that can also convey up-to-the-minute privacy and security status reports to users, regulators and other trusted third parties.

The Office of the Information and Privacy Commissioner of Ontario remains committed to seeking privacy-enhanced technology solutions to the growing digital identity needs of today and tomorrow.

To this end, we hope to encourage greater understanding, participation and dialogue among all stakeholders in the identity world of the essential privacy issues at play, and of the solutions possible.

We call upon all stakeholders and technology developers, in particular, to develop trusted mechanisms for assuring widespread and enduring user confidence in the privacy and security of their identity data in the Web 2.0 world of the future.

Let the dialogue begin!

INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

2 Bloor Street East, Suite 1400

Toronto, Ontario M4W 1A8 Canada

Tel: 416 326 3333

Fax: 416 325 9195

1 800 387 0073

TTY: 416 325 7539

www.ipc.on.ca