IDIS (2008) 1:89–108
DOI 10.1007/s12394-008-0005-z

Privacy in the clouds

Ann Cavoukian

Received: 22 July 2008 / Accepted: 10 September 2008 / Published online: 18 December 2008
© Identity Journal Limited 2008

Abstract Informational self-determination refers to the right or ability of individuals to exercise personal control over the collection, use and disclosure of their personal data by others. The basis of modern privacy laws and practices around the world, informational privacy has become a challenging concept to protect and promote in a world of ubiquitous and unlimited data sharing and storage among organizations. The paper advocates a "user-centric" approach to managing personal data online. However, user-centricity can be problematic when the user—the data subject—is not directly involved in transactions involving the disclosure, collection, processing, and storage of their personal data. Identity data is increasingly being generated, used and stored entirely in the networked "Cloud", where it is under control of third parties. The paper explores possible technology solutions to ensure that individuals will be able to exercise informational self-determination in an era of network grid computing, exponential data creation, ubiquitous surveillance and rampant online fraud. The paper describes typical "Web 2.0" use scenarios, suggests some technology building blocks to protect and promote informational privacy online, and concludes with a call to develop a privacy-respective information technology ecosystem for identity management. Specifically, the paper outlines four fundamental technological approaches to help assure widespread and enduring online participation, confidence and trust in the information society.

Keywords Cloud computing · Identity management · Informational self-determination · Online trust · PETs · Privacy · Privacy-enhancing technologies · User-centric identity · Web 2.0

A. Cavoukian (✉)
Office of the Information and Privacy Commissioner, Toronto, ON, Canada
e-mail: Commissioner@ipc.on.ca

Introduction

Informational self-determination refers to the right or ability of individuals to exercise personal control over the collection, use and disclosure of their personal information by others.[1] It forms the basis of modern privacy laws and practices around the world.

All organizations that collect and use personal data of individuals must accommodate the legitimate interests of these individuals. Organizations can do this, for example, by being open and accountable about their data management practices, by seeking informed consent from individuals, and by providing them with credible access and redress mechanisms. Beyond personal privacy, at stake is the confidence and trust of all individuals, consumers, and citizens in today's evolving information society.

At the Office of the Information and Privacy Commissioner of Ontario (IPC), we have long advocated a strong role for individuals to manage their personal information, They can do this by exercising their privacy rights under Ontario law, by becoming better informed about privacy risks and choices, and by using privacy-enhancing technologies (PETs). PETs empower individuals in many ways; they can minimize the disclosure and (mis)use of personal data, and help secure that data from unauthorized use by others.

Informational self-determination has become a challenging concept to promote and to protect in a world of ubiquitous and unlimited data passing from individuals to organizations, between individuals, and among organizations world-wide. The "Web 2.0" participatory phenomenon is just the latest stage of an ongoing revolution in information and telecommunications technologies (ICTs) that is generating, transmitting and storing data volumes at ever-accelerating growth rates. A large majority of this data is personally identifiable; a greater and growing share is under the control of third parties, in foreign jurisdictions.[2] Practical obscurity—the basis for privacy norms throughout history—is fast disappearing. At the same time, accountability for irresponsible data privacy practices has become more obscure.

Thanks to the use of unique identifiers and sophisticated matching algorithms, our digital interactions and tracks are being gathered together, bit by bit, megabyte by megabyte, terabyte by terabyte, into personas, profiles and similar composite digital entities—virtual representations of us, available in a hundred thousand locations at once. Identity-based systems will provide us with extraordinary new services, new conveniences, new efficiencies, and many other undreamt benefits. At the same time, new risks and threats are emerging from this digital cornucopia. Identity fraud and theft are the diseases of the Information Age made possible by the surfeit of personal data in circulation, along with new forms of discrimination and social engineering made possible by asymmetries of data, information and knowledge.[3]

Personal data, be it biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational or reputational, is the stuff that

[1] On the origins of informational self-determination, see Jóri 2007 and Virtual Privacy Office 2008.

[2] For current statistics, see EMC-IDC Research 2008.

[3] See Solove 2004, 2007.

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[4]—that is, everywhere except on their own personal computing devices?

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

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[5], 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.[6,7]

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

[4] 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. *Cloud computing* means Internet ('cloud') based development and use of computer technology. It is a style of computing where IT-related capabilities are provided "as a service", allowing users to access technology-enabled services "in the cloud" without knowledge of, expertise with, or control over the technology infrastructure that supports them. For a fuller discussion, see Wikipedia entry on "cloud computing".

[5] See O'Reilly 2005.

[6] See: Wired Interview 2007; J. Markoff 2007; and The Economist 2006.

[7] For a good discussion, see Carr 2008.

the personal computer or the opening of the Internet—will match the upheaval that lies just over the horizon."[8]

The new digital ecosystem will also present complex security and privacy challenges.[9] 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. "**Cloud Computing**" in which users rely heavily on data and software that reside on the Internet.[10] 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.

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.[11] 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;

[8] Carr 2005, pp. 67–73.

[9] For a discussion see Cavoukian 2005 and 2006 and Cassasa-Mont et al. 2007.

[10] See Wilder 2006.

[11] See Grossman 2006. For stats, see: Sifry 2007 and OECD 2008.

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; and
5. **Simpler devices**: With data and the software being stored in the Cloud, users do not 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.

A typical Internet user has provided some type of personal information to dozens, if not hundreds, of different websites. Counting cookies and IP addresses as personal information, Internet users have left behind personally identifiable information *everywhere* they have 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.[12]

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.[13]

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

[12] See Story 2008 and O'Harrow 2006.

[13] For a discussion of the need for a globally interoperable "identity metasystem" see Cavoukian 2006.

'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.[14]

Today, more than 10,000 websites support OpenID log-ins, and an estimated 350 million OpenID-enabled URLs currently exist.[15]

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

[14] See: www.openid.net and http://en.wikipedia.org/wiki/Openid.

[15] Details at http://openid.net/wp-content/uploads/2008/03/openid-final-press-release-20080207.doc.

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.[16]

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.[17] 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.[18]

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

[16] Exciting work on minimal disclosure tokens is being carried out under the IDEMIX (Identity mixing) project at: www.zurich.ibm.com/pri/projects/idemix.html and www.zurich.ibm.com/news/07/idemix.html and also by Credentica's U-Prove product at www.credentica.com and and www.emediawire.com/releases/2007/2/emw504697.htm.

[17] See, for example, M-Alliance payment solutions at: http://cordis.europa.eu/ictresults/index.cfm/section/news/tpl/article/BrowsingType/Features/ID/551 and mPayment service offerings at: www.netsize.com/products/mpayment.aspx and Diversinet products and services at: www.diversinet.com.

[18] A comprehensive list of breaches is maintained at the Data Loss Archive and Database at: http://attrition.org/dataloss/.

prescriptions. It would also enable a patient to use an online portal with a federated identity system to quickly and safely access their medical information, whether it is 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.[19]

5. Identity and Trust in Virtual Worlds

Over the past years, 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.[20] 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.[21]

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 goals 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

[19] For an account of the potential problems associated with health records, see World Privacy Forum 2008. For principled approaches to building privacy into health record systems, see Center for Democracy and Technology 2008 and also Markle Foundation Connecting for Health 2008.

[20] www.secondlife.com and www.there.com and www.worldofwarcraft.com.

[21] See: U.S. Congress 2008, Subcommittee on Telecommunications and the Internet; Duranske 2008 and Noguchi 2005. Lawrence Lessig (2006) had much to say about virtual worlds in Code Version 2.0. For an interesting discussion about the identities of corporate avatars, see Ian Kerr and Bornfreund 2005.

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.[22]

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 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

[22] See Cavoukian 2006 (October). Important work on usability is being carried out by the Carnegie-Mellon University Usable Privacy and Security (CUPS) Laboratory at: http://cups.cs.cmu.edu/.

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 intellectual property 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 are stable and enduring.[23]

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 a 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, birth date, 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.[24]

[23] Considerable standards work is underway. See for example, list of ICT Standards Consortia, at www.cen.eu/cenorm/businessdomains/businessdomains/isss/consortia/index.asp. In the identity space, see: Project Concordia http://projectconcordia.org/; Federation for Identity and Cross-Credentialing Systems (FiXs) www.fixs.org; Open Source Identity Systems (OSIS) http://osis.idcommons.net; Higgins: Open Source identity Framework www.eclipse.org/higgins/; Information Card Foundation: http://informationcard.net/. A good overview and commentary is provided by Dan Blum 2008.

[24] An excellent overview of the concept of personal data is provided by the E.U. Article 29 Data Protection Working Party 2007.

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.[25]

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.[26] 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[27] 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.

[25] In 2006 the Information and Privacy Commissioner of Ontario 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.

[26] See, for example, Microsoft Corp 2006. The Identity Metasystem: Towards a Privacy-Compliant Solution to the Challenges of Digital Identity (October 2006), at: www.identityblog.com/wp-content/resources/Identity_Metasystem_EU_Privacy.pdf.

[27] See Further Reading for key papers treating PETs and privacy-enhanced identity management technologies and systems.

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.[28]
- **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.[29]
- **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 and to which the user had consented.

[28] See Wikipedia entries for “federated identity” and “single sign-on”.

[29] See, for example, E-Health Europe 2008.

- **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.[30] 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; and
- 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

[30] An overview is provided by Lunt et al. 2007.

identity data, similar to digital rights management technologies for intellectual property.[31]

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.[32]

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."[33]

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.[34]

[31] For a seminal discussion of how DRM technologies can be applied to privacy, see Korba and Kenny 2002.

[32] Privacy testing and certification of consumer technologies will be critical to assuring trust. See the European Privacy Seal ("EuroPriSe") for IT Products and IT-Based Services at: www.european-privacy-seal.eu/.

[33] For a thorough discussion of intelligent agents, see PISA Project 2003 and Ian Kerr 2001 and 2004. A list of internet resources about agents can be found at: http://ai.ijs.si/mezi/agents/agents.html.

[34] Some notable privacy audit tools and technologies include: SPARCLE (Server Privacy ARrchitecture and CapabiLity Enablement) policy workbench. SPARCLE was created to help organizations manage the privacy of the personal information they store in their systems. Now, broader applicability of the technology to other types of policies including security, systems management, autonomic computing, and compliance auditing is envisioned: http://domino.research.ibm.com/comm/research.nsf/pages/r.security.innovation2.html SPARCLE is based on the Enterprise Privacy Authorization Language W3C specification (EPAL 1.2). For a discussion about the role of IT security standards in helping to protect personal information, see: Giovanni Iachello 2003. For general privacy audit standards, see Canadian Institute of Chartered Accountants (CICA) and American Institute of Certified Public Accountants (AICPA), Generally Accepted Privacy Principles (GAPP) and related resources at: www.cica.ca/3/6/5/2/9/index1.shtml and at http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles/. A good concordance of privacy principles and how they intersect with major privacy laws was prepared by International Security, Trust and Privacy Alliance (ISTPA) 2007.

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!

Acknowledgements The author would like to acknowledge and thank IBM Research Systems & Software experts, in particular, Dr. Jan Camenisch, Anthony Nadalin, Michael R. Nelson and Dr. Michael Waidner for their contribution. The author also acknowledges the contribution of Fred Carter, Senior Privacy & Technology Advisor, Office of the Information and Privacy Commissioner of Ontario, in the preparation of this paper.

References

Blum D. Identity interoperability, standards, and the state of adoption. Presentation for the ID Trust (04 March 2008) at: http://middleware.internet2.edu/idtrust/2008/slides/01-blum-standards.ppt.

Carr NG. The end of corporate computing. MIT Sloan Management Review, Spring; 2005, pp. 67–73.

Carr NG. The big switch: Rewiring the world, from Edison to Google. W.W. Norton & Co.; 2008 at: www.nicholasgcarr.com/bigswitch/.

Cavoukian A. Identity theft revisited: Security is not enough. (Sept 2005) at: www.ipc.on.ca/images/Resources/idtheft-revisit.pdf.

Cavoukian A. 7 laws of identity: The case for privacy-embedded laws of identity in the digital age. (October 2006) at: www.ipc.on.ca/images/Resources/up-7laws_whitepaper.pdf.

Cavoukian A. Privacy and the open networked enterprise. (December 2006) at: www.ipc.on.ca/images/Resources/up-opennetw.pdf.

Casassa-Mont M, Pearson S, Bramhall P. Towards accountable management of identity and privacy: Sticky policies and enforceable tracing services. (19 March 2003) at: www.hpl.hp.com/techreports/2003/HPL-2003-49.pdf.

Casassa-Mont M, Pearson S, Novoa M. Securing information transfer in distributed computing environments. In: IEEE Security & Privacy; Nov/Dec 2007, pp. 34–42.

Center for Democracy and Technology. Privacy and security principles for health information technology. (24 June 2008) at: http://cdt.org/publications/policyposts/2008/9.

Duranske B. Congress holds first hearing on virtual worlds. Virtually blind (01 April 2008) at: http://virtuallyblind.com/2008/04/01/congress-virtual-worlds/.

E-Health Europe. German ID card to allow pseudonyms. (27 Feb 2008) at: www.ehealtheurope.net/news/3505/german_id_card_to_allow_pseudonyms.

EMC-IDC Research. Expanding digital universe: A forecast of worldwide information growth through 2011. (March 2008) at: www.emc.com/about/destination/digital_universe/.

European Union. Article 29 Data Protection Working Party. Opinion N° 4/2007 on the concept of personal data. (20 June 2007) at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

Grossman L. Time's person of the year: You. Time magazine (13 Dec 2006) at: www.time.com/time/magazine/article/0,9171,1569514,00.html.

Iachello G. Protecting personal data: Can IT security management standards help? (Jan 2003) at: www.ipc.on.ca/images/Resources/up-PPPP038.pdf.

International Security, Trust and Privacy Alliance (ISTPA). Analysis of privacy principles: Making privacy operational, version 2.0. (May 2007) at: www.istpa.org/pdfs/ISTPAAnalysisofPrivacyPrinciplesV2.pdf.

Jóri A. Data protection law—an introduction. (2006–2007) at: www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.SecondGeneration.
Kerr I. Ensuring the success of contract formation in agent-mediated electronic commerceElectronic Commerce Research Journal20011183–202at: http://iankerr.ca/files/kerr-agent-mediated.pdf A list of internet resources about agents can be found at: http://ai.ijs.si/mezi/agents/agents.html.
Kerr I. Bots, babes and the Californication of commerceOttawa Law and Technology Journal20041285–325at: http://iankerr.ca/files/BotsBabesandtheCalifornicationofCommerce.pdf.
Kerr I, Bornfreund M. Buddy bots: How Turing's fast-friends are under-mining consumer privacy. In: Presence: Teleoperators and Virtual Environments; 2005. pp. 647–655, at: http://iankerr.ca/files/Kerr-Bornfreund-Buddybots.pdf.
Korba L, Kenny S. Towards meeting the privacy challenge: Adapting DRMWashington, D.C.2002 ACM Workshop on Digital Rights Management2002(November) at: http://iit-iti.nrc-cnrc.gc.ca/iit-publications-iti/docs/NRC-44956.pdf.
Lessig L. Code: And other laws of cyberspace, version 2.0. 2006 (Persueus) at http://codev2.cc/.
Lunt T et al. Technology and privacy. Montreal: 29th International Conference of Privacy and Data Protection Commissioners; 2007 (September) at: www.privacyconference2007.gc.ca/workbooks/pres_plenary1_02_lunt_e.pdf.
Markle Foundation Connecting for Health. Technology companies, providers, health insurers and consumer groups agree on framework for increasing privacy and consumer control over personal health records. (25 June 2008) at: www.connectingforhealth.org/news/pressrelease_062508.html.
Markoff J. Software via the Internet: Microsoft in 'Cloud' computing. New York Times; (3 September 2007) at: www.nytimes.com/2007/09/03/technology/03cloud.html?_r=2.
Microsoft Corp. The identity metasystem: Towards a privacy-compliant solution to the challenges of digital identity. (October 2006), at: www.identityblog.com/wp-content/resources/Identity_Metasystem_EU_Privacy.pdf.
Noguchi Y. Self 2.0: Internet users put a best face forward. The Washington Post; (22 November 2005), at: www.washingtonpost.com/wp-dyn/content/article/2005/11/21/AR2005112101787.html.
O'Harrow R. No Place to Hide. Free; 2006, at: /www.noplacetohide.net/.
O'Reilly T. What is Web 2.0: Design patterns and business models for the next generation of software. (30 September 2005) at: www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.
Organization for Economic Cooperation and Development (OECD). Measuring user-created content: Implications for the "ICT access and use by households and individuals" surveys. (30 January 2008) at www.oecd.org/dataoecd/44/58/40003289.pdf.
PISA Project. Handbook of privacy and privacy-enhancing technologies—the case of intelligent software agents. The Hague; 2003 at: www.cbpweb.nl/downloads_technologie/PISA_handboek.pdf.
Schmidt E. Wired interview. (4 September 2007) at www.wired.com/techbiz/people/news/2007/04/mag_schmidt_trans.
Sifry D. State of the blogosphere/state of the live Web. (April 2007) at: www.sifry.com/stateoftheliveweb/ and www.sifry.com/alerts/archives/000493.html.
Solove DJ. The digital person: Technology and privacy in the information age. NYU; 2004 at: http://docs.law.gwu.edu/facweb/dsolove/Digital-Person/index.htm.
Solove DJ. The future of reputation: Gossip, rumor, and privacy on the Internet. Yale; 2007 at: http://docs.law.gwu.edu/facweb/dsolove/Future-of-Reputation/.
Story L. To aim ads, Web is keeping closer eye on you. New York Times; (10 March 2008) www.nytimes.com/2008/03/10/technology/10privacy.html?_r=4&pagewanted=1&hp.
The Economist. Don't bet against the internet. (November 2006) at: www.economist.com/theworldin/business/displayStory.cfm?story_id=8133511.
United States Congress. Subcommittee on telecommunications and the Internet. "Online virtual worlds: Applications and avatars in a user-generated medium" at: http://energycommerce.house.gov/cmte_mtgs/110-ti-hrg.040108.VirtualWorlds.shtml.
Virtual Privacy Office. Informational self-determination—what does that mean? (2008) at: www.datenschutz.de/privo/recht/grundlagen/.
Wilder G. The information factories. Wired magazine; (October 2006) at: www.wired.com/wired/archive/14.10/cloudware_pr.html.
World Privacy Forum. Personal health records: Why many PHRs threaten privacy. (February 2008) at: www.worldprivacyforum.org/pdf/WPF_PHR_02_20_2008fs.pdf and Consumer Advisory: www.worldprivacyforum.org/pdf/WPF_PHRConsumerAdvisory_02_20_2008fs.pdf.

Privacy Enhancing Technologies (PETs)

Cavoukian A. Information and privacy commissioner of Ontario & Dutch registratierkamer, Privacy-Enhancing Technologies: The Path to Anonymity Volume I—August 1995: www.ipc.on.ca/index.asp?layid=86&fid1=329 Volume II—August 1995: www.ipc.on.ca/images/Resources/anoni-v2.pdf.

Dutch Interior Ministry. Privacy-enhancing technologies. White paper for decision-makers (December 2004) at: www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf.

European Commission Supports PETs: Promoting Data Protection by Privacy Enhancing Technologies, (2 May 2007) http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=3402.

European Commission steps up efforts in Privacy Enhancing Technologies, (12 Dec 2007) http://cordis.europa.eu/fetch?CALLER=EN_NEWS&ACTION=D&SESSION=&RCN=28802.

EU PRIME Project / UK Knowledge Transfer Networks (KTN). A fine balance: Privacy enhancing technologies: How to create a trusted information society. (21 November 2007) at www.petsfinebalance.com/docrepo/Fine%20Balance%20London%20FinalReport%20FINAL%20VERSION.pdf.

EU FIDIS Project. Identity and impact of privacy enhancing technologies. (May 2007) www.fidis.net/fileadmin/fidis/deliverables/fidis-wp13-del13.1.identity_and_impact_PET.pdf.

EU PRIME Project. Privacy-enhancing identity management, White paper v2. (June 2007) at https://www.prime-project.eu/prime_products/whitepaper/PRIME-Whitepaper-V2.pdf.

Information on EU funding for Information and Communication Technologies (ICT) research under the Seventh Framework Programme (FP7) accessed on August 12, 2008 http://cordis.europa.eu/fp7/ict/.

UK Information Commissioner. Data protection technical guidance note: Privacy enhancing technologies. (November 2006) at http://tinyurl.com/23b6kc.

Organisation for Economic Co-operation and Development (OECD)

At a Crossroads: "Personhood" and the Digital Identity in the Information Society. STI Working Paper 2007/7. (29 February 2008). www.oecd.org/dataoecd/31/6/40204773.doc.

Closing remarks by Angel Gurría, OECD ministerial meeting on the future of the Internet economy, (20 June 2008) affirming support for OECD privacy principles, at www.oecd.org/document/8/0,3343,en_2649_34487_40863240_1_1_1_1,00.html.

Inventory of Privacy-Enhancing Technologies (PETs). DSTI/ICCP/REG(2001)1/FINAL (January2002) at: www.olis.oecd.org/olis/2001doc.nsf/LinkTo/dsti-iccp-reg(2001)1-final.

OECD Seoul. Declaration on roadmap for the future of the Internet economy. (17–18 June 2008) at www.oecd.org/dataoecd/49/28/40839436.pdf.

Recommendation on Electronic Authentication and Guidance for Electronic Authentication. (June 2007). www.oecd.org/document/7/0,3343,en_2649_33703_38909639_1_1_1_1,00.html. www.oecd.org/dataoecd/32/45/38921342.pdf.

Workshop on Digital Identity Management (IDM)—Trondheim, Norway, 8–9 May 2007 www.oecd.org/document/41/0,3343,en_2649_34255_38327849_1_1_1_1,00.html. Workshop *Final Report* www.oecd.org/dataoecd/30/52/38932095.pdf.

Privacy/Trust Standards

Borking J. Privacy Standards for Trust. (October 2005) www.privacyconference2005.org/fileadmin/PDF/borking.pdf.

Borking J. Privacy rules, a steeple chase for systems architects. www.w3.org/2006/07/privacy-ws/papers/04-borking-rules/.

Kenny S, Borking J. The value of privacy engineering. Refereed Article, The Journal of Information, Law and Technology (JILT) 2002;(1). www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_1/kenny/.

Security Assertion Markup Language (SAML). SAML Executive Summary: www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf. Wikipedia entry: http://en.wikipedia.org/wiki/SAML.

User Centric Identity Management: An Oxymoron Or The Key To Getting Identity Management Right?, Presentation by Malcolm Crompton, Information Integrity Solutions Pty Ltd; (April 2008): www.iispartners.com/NZ_background_paper_29.04.08.pdf. Presentation: www.iispartners.com/NZ_presentation_ 29.04.08.pdf.

29th International Data Protection and Privacy Commissioners' Conference. (Sept 2007), Resolution on development of international standards. www.privacyconference2007.gc.ca/Global%20Standards%20Resolution%20-%20English.pdf.

29th International Conference of Data Protection and Privacy Commissioners. (September 2007) Terra Incognita standards workshop–workbook: www.privacyconference2007.gc.ca/workbooks/Terra_Incognita_workbook5_bil.pdf.

Online Identity and Privacy: Issues and Recommendations

CDT "Privacy principles for the development of user controls for behavioral targeting" (March 2008) at: www.cdt.org/privacy/pet/Privacy_Controls_IPWG.pdf.

European Network and Information Security Agency (ENISA). Security issues and recommendations for online social networks. Hogben G, editor. (October 2007). www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf.

European Union. Article 29 data protection working party. Opinion 1/2008 on data protection issues related to search engines (4 April 2008). http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf.

International Working Group on Data Protection in Telecommunications. Report and guidance on privacy in social network services—"Rome Memorandum"—43rd meeting, 2008; 3–4 March, Rome (Italy). www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491.

Office of the Privacy Commissioner of Canada. Identity, privacy and the need of others to know who you are: A discussion paper on identity issues (September 2007). www.privcom.gc.ca/information/pub/ID_Paper_e.pdf.

Pew Internet & American Life Project. Digital footprints: Online identity management and search in the age of transparency (December 2007). http://cdn.sfgate.com/chronicle/acrobat/2007/12/13/pip_digital_fp_2007.pdf.

Pew Internet & American Life Project. Seeding the cloud: What mobile access means for usage patterns and online content (March 2008), at www.pewinternet.org/pdfs/PIP_Users.and.Cloud.pdf.

Online Computer Library Center. Sharing, "Privacy and trust in our networked world" (Sept 2007), at: www.oclc.org/reports/sharing/default.htm. Section on Privacy, Security and Trust at: www.oclc.org/reports/pdfs/sharing_part3.pdf.

Wright D, Gutwirth S, Friedewald M, Vildjiounaite E, Punie Y (Eds.). Safeguards in a World of Ambient Intelligence (Springer, 2008). www.springer.com/computer/database+management+&+information+retrieval/book/978-1-4020-6661-0. Chapter 1: www.springerlink.com/content/j23468h304310755/fulltext.pdf.

Papers by Ann Cavoukian, Ph.D., Information and Privacy Commissioner/ Ontario

An Internet Privacy Primer: Assume Nothing (August 2001). Joint paper with Microsoft Canada. www.ipc.on.ca/images/Resources/primer-e.pdf.

"Best Practices for Online Privacy Protection" (June 2001). www.ipc.on.ca/images/Resources/bpon-e.pdf.

Biometric Encryption: A positive-sum technology that achieves strong authentication, security AND privacy, at: www.ipc.on.ca/index.asp?navid=46&fid1=608.

Concerns & Recommendations Regarding Government Public Key Infrastructures for Citizens (December 2002): http://www.ipc.on.ca/index.asp?navid=46&fid1=339.

Contactless Smart Card Applications: Design tool and privacy impact assessment. Joint paper with the Advanced Card Technology Association of Canada (ACT Canada), (May 2007): wwww.ipc.on.ca/images/Resources/up-act_pia.pdf.

Cross-National Study of Canadian and U.S. Corporate Privacy Practices. IPC-commissioned Ponemon Institute study that benchmarks the corporate privacy practices of Canadian and U.S. companies (May 2004): www.ipc.on.ca/images/Resources/cross.pdf.

EPAL Translation of the Freedom of Information and Protection of Privacy Act. Joint white paper with IBM Tivoli Software on Enterprise privacy authorization language (EPAL) (March 2004): www.ipc.on.ca/images/Resources/up-EPAL_FI1.pdf. EPAL site: www.zurich.ibm.com/pri/projects/epal.html.

"Fingerprint Biometric Systems: Ask the right questions before you deploy" (July 2008). www.ipc.on.ca/images/Resources/fingerprint-biosys.pdf.

"Global Privacy Standard" (Nov 2006). www.ipc.on.ca/images/Resources/up-gps.pdf.

Identity Theft Revisited: Security is not enough (September 2005). www.ipc.on.ca/images/Resources/idtheft-revisit.pdf.

"Incorporating Privacy into Marketing and Customer Relationship Management". A joint report with the Canadian Marketing Association. (May 2004): http://www.ipc.on.ca/images/Resources/priv-mkt.pdf.

Intelligent Software Agents: Turning a privacy threat into a privacy protector. Joint project with the Registratierkamer, The Netherlands. (April 1999). www.ipc.on.ca/images/Resources/up-isat.pdf.

National Security in a Post-9/11 World: The rise of surveillance.. the demise of privacy? (May 2003) at: www.ipc.on.ca/images/Resources/up-nat_sec.pdf.

Privacy and the Open Networked Enterprise (June 2005). Outlines the major privacy and information management challenges facing all enterprises in the next generation, at: www.ipc.on.ca/images/Resources/up-opennetw.pdf.

Privacy and Digital Rights Management (DRM): An Oxymoron? (October 2002). www.ipc.on.ca/images/Resources/up-1drm.pdf.

Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines). (June 2006): www.ipc.on.ca/images/Resources/up-1rfidgdlines.pdf. Practical Tips for Implementing RFID Privacy Guidelines: www.ipc.on.ca/images/Resources/up-rfidtips.pdf.

P3P and Privacy: An update for the privacy community. Joint paper with the center for democracy and technology (March 2000), at: www.ipc.on.ca/images/Resources/p3p.pdf.

"RFID and Privacy: Guidance for health-care providers" (January 2008) www.ipc.on.ca/images/Resources/up-1rfid_HealthCare.pdf. News Release: www.ipc.on.ca/images/Resources/up-2008_01_23_rfidheathcare.pdf.

"Security Technologies Enabling Privacy (STEPs): Time for a paradigm shift" (June 2002) www.ipc.on.ca/images/Resources/steps.pdf. "Commissioner issues challenge to technologists: Take the next STEP" (January 2002). www.ipc.on.ca/index.asp?layid=86&fid1=333.

Should the OECD Guidelines Apply to Personal Data Online? (Sept 2000). www.ipc.on.ca/images/Resources/up-oecd.pdf.

Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology. (February 2004): www.ipc.on.ca/images/Resources/up-rfid.pdf.

"Transformative Technologies Deliver both Security and Privacy: Think positive-sum not zero-sum" (July 2008). www.ipc.on.ca/images/Resources/trans-tech-handout.pdf.

Web Seals: A review of online privacy programs. Joint paper with the federal privacy commissioner of Australia (Sept 2000), www.ipc.on.ca/images/Resources/up-seals.pdf

7 Laws of Identity: The case for privacy-embedded laws of identity in the digital age. (October 2006): www.ipc.on.ca/images/Resources/up-7laws_whitepaper.pdf. Booklet: www.ipc.on.ca/images/Resources/up-7laws_brochure.pdf.