7 LAWS OF IDENTITY

THE CASE FOR PRIVACY-EMBEDDED LAWS OF IDENTITY IN THE DIGITAL AGE

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

Commissioner Ann Cavoukian gratefully acknowledges the work of Fred Carter, Senior Policy and Technology Advisor at the IPC, in the preparation of this paper.

TABLE OF CONTENTS

BACKDROP

The existing identity infrastructure of the Internet is no longer sustainable. The level of fraudulent activity online has grown exponentially over the years and is now threatening to cripple e-commerce. Something must be done now before consumer confidence and trust in online activities are so diminished as to lead to its demise. Enter the 7 Laws of Identity: could this be the answer? Read on.

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

INTRODUCTION

This paper recognizes and is inspired by the "7 Laws of Identity" formulated on an open blog by a global community of experts through the leadership of Kim Cameron, Chief Identity Architect at Microsoft.

The Office of the Information and Privacy Commissioner of Ontario is convinced that the "7 Laws" (*a.k.a.* "technologically-necessary principles of identity management") will profoundly shape the architecture and growth of a universal identity metasystem. The resulting "Identity Big Bang" will hopefully enable the Internet to evolve to the next level of trust and capability.

A universal identity metasystem will also have profound impacts on privacy since the digital identities of people – and the devices associated with them – constitute personal information. Care must be taken that a universal, interoperable identity metasystem does not get distorted and become an infrastructure of universal surveillance.

We have always advocated that privacy be built into the design and operation of information systems and technologies. We do this by applying the privacy principles expressed in the "Fair Information Practices" in a systematic way. (See Appendix A)

We are struck by the many similarities between the 7 Laws of Identity and the fair information practices. The two sets of fundamental principles are highly complementary and inform each other.

This document is the result of our "mapping" fair information practices over the 7 Laws of Identity to explicitly extract their privacy-protective features. The result, which we call the "privacy-embedded" Laws of Identity, is a commentary on the Laws that "teases-out" the privacy implications, for all to consider.

The privacy-embedded Laws of Identity are intended to inject privacy considerations into discussions involving identity – specifically, into the emerging technologies that will define an interoperable identity system.

We believe that privacy is woven through the 7 Laws and that when the Laws are applied, exciting new privacy options will become possible. However, there is nothing inevitable about privacy-enhanced identification and authentication options. An identity metasystem (described by the 7 Laws) is a necessary but not sufficient condition for privacy-enhancing options to be developed.

The missing ingredients are knowledge and desire. If privacy design options for identity systems can be identified and promoted, then it is possible that a universal identity metasystem will emerge that has built-in respect for privacy and data protection, before it's too late.

IDENTITY AND PRIVACY

Identity and privacy are closely related. Generally speaking, when your identity is not known, you tend to have more privacy. When you pay cash for a coffee, your "identity" is that of an anonymous consumer. When you buy coffee with an anonymous pre-paid coffee card, your "identity" becomes that of a loyal patron. But, when your name and address are linked to a pre-paid coffee card, all of your coffee purchases may be linked to you, as an identifiable individual. Information that can be linked to an identifiable individual is considered to be personal information.

Privacy refers to the claim or right of individuals to exercise a measure of control over the collection, use and disclosure of their personal information. When your personal information is mishandled, your privacy interests are engaged.

Protecting and promoting individual privacy is a real challenge in an era of exponential creation, networking and duplication of data, most of which is identifiable in nature. There is more personal information out there than ever before, and most of it is controlled by others. Increasingly we have little control over our own information.

Identification requirements are everywhere, and increasing. We all have multiple identities which need to be managed. In the online digital environment, however, the identity challenges are greater, since identification demands are becoming more frequent. Increasingly, more and more granular information is being collected about us by others, and this data is being used in novel ways, for novel purposes – not all of which benefit the individual.

There is a growing disjunct with the bricks-and-mortar world where, for example, we can often demonstrate our identity (or credentials) by simply waving an ID document for visual inspection. But in the faceless online world, our identification "credential" is often recorded in databases, compared or collated with other data, and stored indefinitely for further uses.

At the same time, the identity of other entities online is becoming harder to verify. We often simply do not know who we are truly dealing with online, or how accountable they are with respect to the handling of our personal information.

DIGITAL IDENTITY AND PRIVACY: THE CHALLENGE

For users and businesses alike, the Internet continues to be increasingly valuable. More people are using the web for everyday tasks, from shopping, banking, and paying bills to consuming media and entertainment. E-commerce opportunities are growing, with businesses delivering more services and content across the Internet, communicating and collaborating online, and inventing new ways to connect with each other.

But as the value of what people do online has increased, the Internet itself has become more complex, vulnerable, and dangerous. Online identity theft, fraud, and privacy concerns are on the rise, stemming from increasingly sophisticated practices such as "phishing," "spear-phishing," and pharming. Keeping track of multiple accounts, passwords and authentication methods is difficult and frustrating for users. "Password fatigue" results in insecure practices such as re-using the same account names and passwords at many sites.

THE NEED FOR IDENTITY MANAGEMENT

Identity management is a hot topic these days, but what exactly is it? The term does not have a clearly defined meaning, but technology-based identity management, in its broadest sense, refers to the administration and design of identity attributes, credentials, and privileges.

Identity management may be carried out centrally by others, as in the case of organizations that assign "log on" credentials to individuals to facilitate and control access to critical resources. When you leave the organization, your network identity and associated privileges are revoked by the system administrator. This is often called *enterprise* identity management or, more simply, *provisioning*. Centralized identity management may also occur beyond the enterprise, as when governments issue national identity cards for use in multiple scenarios, or in some online single-sign-on schemes such as Microsoft .Net Passport service.

Another form of identity management is "user-centric" which seeks to place administration and control of identity information directly into the hands of individuals. Examples include network anonymization tools and form fillers that minimize disclosure of personal information, or password managers that securely keep track of different credentials. In the real world, a wallet full of different identity cards is a user-centric form of identity management that allows individuals to choose the appropriate identity credential for the right purposes, such as a coffee card for coffee and a student

ID card for discounts. Individuals can exercise control over how the information on those cards is read and used by others.

A third type of identity management, commonly referred to as "federated," is a hybrid of the two. In such systems, one's identity credentials are divided and spread out among many parties, with users controlling how they are shared and used. Some single sign-on schemes can work this way. The ability to authorize a government agency to share change-of-address information with other departments may be another. The risks to privacy can be offset by careful choice of trusted identity providers, and by greater convenience and efficiencies for users.

All three types of identity management systems are necessary, depending on the context. Identity is highly contextual. Consider that the identities held by a person in the offline world can range from the significant, such as birth certificates, passports, and drivers' licenses, to the trivial, such as business cards or frequent user buyer's cards. People use their different forms of identification in different contexts where they are accepted.

IDENTITY IS CONTEXTUAL

Personal information provided in different contexts will vary. Identities may be used in or out of context. Identities used out of context generally do not bring desired results. For example, trying to use a coffee card to cross a border is clearly out of context. On the other hand, using a bank card at an ATM, a government-issued ID at a border, a coffee card at a coffee shop, and a MS .Net Passport account at MSN Hotmail are all clearly in context.

In some cases, the distinction is less clear. You could conceivably use a government-issued ID at your ATM instead of a bank-issued card, but if this resulted in the government having knowledge of each financial transaction, many people would be uncomfortable. You could use a Social Insurance or Social Security Number as a student ID number, but that has significant privacy implications, such as facilitating identity theft. And you can use a .Net Passport account at some non-Microsoft sites, but few sites chose to enable this; even where it was enabled, few users did so because they felt that Microsoft's participation in these interactions was out of context.

Numerous digital identity systems have been introduced, each with its own strengths and weaknesses. But no one single system meets the needs of every digital identity scenario. Even if it were possible to create one system that did so, the reality is that many different identity systems are in use today, with still more being invented. As a result, the current state of digital identity on the Internet is an inconsistent patchwork of ad hoc solutions that burdens people with different user experiences at every web site, renders the system as a whole fragile, and constrains the fuller realization of the promise of e-commerce.

THE INTERNET'S PROBLEMS ARE OFTEN IDENTITY PROBLEMS

Many of the problems facing the Internet today stem from the lack of a widely deployed, easily understood, secure identity solution.

A comparison between the bricks-and-mortar world and the online world is illustrative: In the bricks-and-mortar world you can tell when you are at a branch of your bank. It would be very difficult to set up a fake bank branch and convince people to do transactions there. But in today's online world it is trivial to set up a fake banking site (or e-commerce site ...) and convince a significant portion of the population that it's the real thing. This is an enormous identity problem. Web sites currently do not have reliable ways of identifying themselves to people, thus enabling impostors to flourish. What is needed is reliable *site-to-user* authentication, which aims to make it as difficult to produce counterfeit services in the online world, as it is to produce them in the physical world.

Conversely, problems identifying users to sites also abound. Username/password authentication is the prevailing paradigm, but its weaknesses are all too evident on today's Internet. Password re-use, insecure passwords, and poor password management practices open a world of attacks, in and of themselves. Combine that with the password theft attacks enabled by counterfeit web sites, and man-in-the-middle attacks, and today's Internet is an attacker's paradise.

The consequences of these problems are severe and growing. The number of "phishing" attacks and sites has skyrocketed. There are reports that online banking activity is declining. Recent regulatory guidance on authentication in online banking reports that "Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation." [FFIEC 05] Consumer trust of the Internet is low and ever-dropping.[NCL 06] Clearly, the status quo is no longer a viable option.

WHAT IS NEEDED: AN IDENTITY METASYSTEM

Given that universal adoption of a single digital identity system or technology is unlikely to occur, a successful and widely deployed identity solution for the Internet requires a different approach – one with the capability to connect existing and future identity systems into an **identity metasystem.** A metasystem, or system of systems, would leverage the strengths of its constituent identity systems, provide interoperability between them, and enable the creation of a consistent and straightforward user interface to all of them. The resulting improvements in cyberspace would benefit everyone, ultimately making the Internet a safer place with the potential to boost e-commerce, combat phishing, and solve other digital identity challenges.

An identity metasystem could make it easier for users to stay safe and in control when accessing resources on the Internet. It could allow users to select from among a portfolio of their digital identities and use them for Internet services of their choice, where they are accepted. A metasystem could enable identities provided by one identity system technology to be used within systems based on different technologies, provided that an intermediary exists that understands both technologies and is capable and trusted to do the needed translations.

It is important to note that the role of an identity metasystem is not to compete with or replace the identity systems that it connects. Rather, a metasystem should rely on the individual systems in play to do its work!

ARCHITECTURE OF A PROPOSED SOLUTION

By definition, in order for a digital identity solution to be successful, it needs to be understood in all the contexts when you may wish to use it to identify yourself. Identity systems are all about identifying yourself (and your things) in environments that are not yours. For this to be possible, both your systems and the systems that are not yours – those where you need to digitally identify yourself – must be able to speak the same digital identity protocols, even if they are running different software on different platforms.

Such a solution, in the form of an identity metasystem, has already been proposed, and some implementations are well under way. The identity metasystem is based upon an underlying set of principles called the "Laws of Identity." The Laws are intended to codify a set of fundamental principles to which a universally adopted, sustainable identity architecture must conform. The Laws were proposed, debated, and refined through a long-running, open, and continuing dialogue on the

Internet by the major players in the identity field. Taken together, the Laws are key to defining the overall architecture of the identity metasystem.

Because these Laws were developed through an open consensus process among experts and stakeholders, they reflect a remarkable convergence of interests, and are non-proprietary in nature. As a result, they have been endorsed and adopted by a long and growing list of industry organizations, associations, and technology developers.

By allowing different identity systems to work together in concert, with a single user experience, and a unified programming paradigm, the metasystem shields users and developers from concerns about the evolution and market dominance of specific underlying systems, thereby reducing everyone's risk and increasing the speed with which the technology can evolve.

It is our sincere belief that the 7 Laws of Identity and the identity metasystem they describe represent significant contributions to improving security and privacy in the online world and, as such, are worthy of closer study, support and broad adoption by the privacy community.

We are particularly struck by the parallels with the fair information practices ("FIPs"), which set forth universal principles that both establish and confer broad rights on *individuals* with respect to the collection, use, and disclosure of their personal information by others, and at the same time set out broad responsibilities for *organizations* in respect to their collection, use and disclosure of personal information. The FIPs have served as the basis for privacy and data protection laws around the world, and yet are versatile enough to be used to guide the design, development and operation of information technologies and systems in a privacy-enhancing manner.

We are impressed with how the Laws of Identity seek to put users in control of their own identities, their personal information, and their online experiences. In the metasystem, users decide how much information they wish to disclose, to whom, and under what circumstances, thereby enabling them to better protect their privacy. Strong two-way authentication of identity providers and relying parties helps address phishing and other forms of fraud. Identities and accompanying personal information can be securely stored and managed in a variety of ways, including via the online identity provider service of the user's choice, or on the user's PC, or in other devices such as secure USB keychain storage devices, smartcards, PDAs, and mobile phones.

Further, the identity metasystem enables a predictable, uniform user experience across multiple identity systems. It extends to and integrates the human user, thereby helping to secure the machine-human channel.

Participants in the identity metasystem may include anyone or anything that uses, participates in, or relies upon identities in any way, including, but not limited to existing identity systems, corporate identities, government identities, Liberty federations, operating systems, mobile devices, online services, and smartcards. Again, the possibilities are only limited by innovators' imaginations.

An example of a universal identity system that did NOT conform with the Laws of Identity is illustrative.

.NET PASSPORT

Until now, Microsoft's best-known identity effort was almost certainly the Passport Network, best known to millions of Internet users as a "single sign-on" identity system that stored users' personal information centrally.

The identity metasystem is different from the original version of Passport in several fundamental ways. The metasystem stores **no** personal information, leaving it up to individual identity providers to decide how and where to store that information. The identity metasystem is not an online identity provider for the Internet; indeed, it provides a means for all identity providers to co-exist with and compete with one another – all having equal standing within the metasystem. And while Microsoft charged companies to use the original version of Passport, no-one will be charged to participate in the identity metasystem.

In fairness, the Passport system itself has evolved in response to these experiences. It no longer stores personal information other than username/password credentials. Passport is now an authentication system targeted at Microsoft sites and those of close partners – a role that is clearly in context, and one which users and partners are more comfortable. Passport and MSN plan to implement support for the identity metasystem as an online identity provider for MSN and its partners. Passport users will receive improved security and ease of use, and MSN Online partners will be able to interoperate with Passport through the identity metasystem.

An example of one desktop application, currently in development, that does embody the 7 Laws of the identity metasystem is also illustrative.

CARDSPACE AND INFORMATION CARDS

Microsoft, among others, is building user software that conforms to the 7 Laws of the identity metasystem. The "Cardspace" identity selector is a Windows component that provides the consistent user experience required by the identity metasystem. It is specifically hardened against tampering and spoofing to protect the end user's digital identities and maintain end-user control. Each digital identity managed in Cardspace (comparable to a virtual card holder) is represented by a visual "information card" in the user interface. The user selects identities represented by information cards to authenticate to participating services.

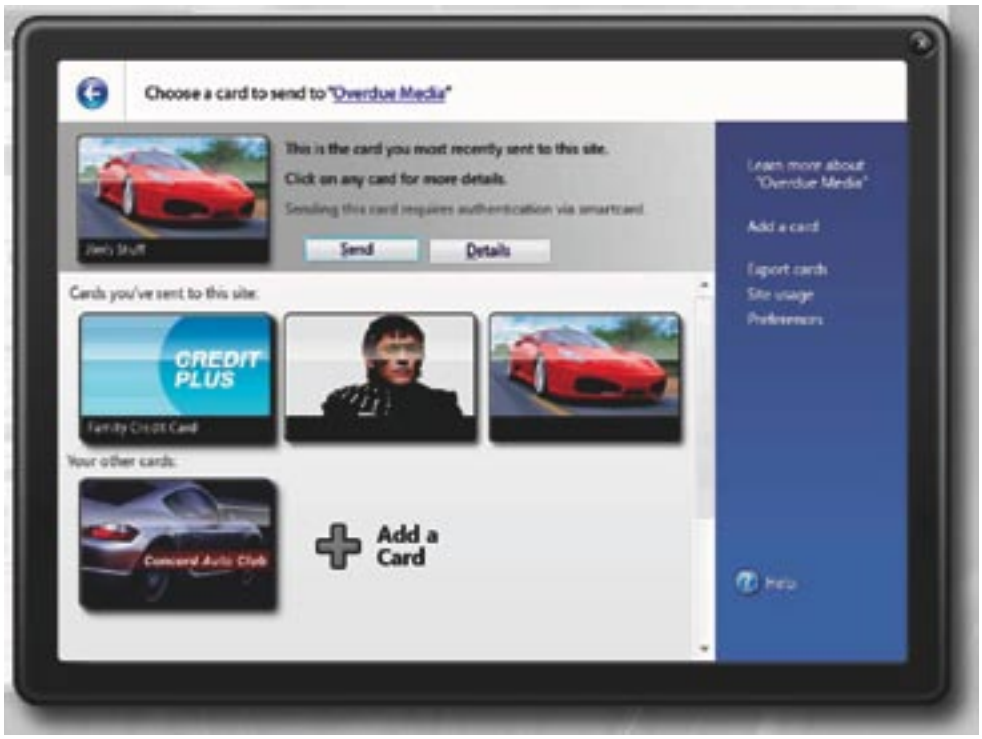

Figure 1: Identity Selector Screen: Information Cards

Many identity attacks succeed because the user was fooled by something presented on the screen, not because of insecure communication technologies. For example, phishing attacks occur not in the secured channel between web servers and browsers — a channel that might extend thousands of miles — but in the two or three feet between the browser and the human who uses it. The identity metasystem, therefore, seeks to empower users to make informed and reasonable identity decisions by enabling the use of a consistent, comprehensible, and self-explanatory user interface for making those choices.

As Figure 1 illustrates, users can be in control of their identity interactions (see Laws 1 & 2) by being able to choose which identities to use at which services, by knowing what information will be disclosed to those services if they use them, and by being informed how those services will use the information they disclose. To be in control, you must first be able to understand the choices you are presented with (see Laws 6 & 7). Unless users can be brought into the identity solution as informed, functioning components of the solution, able to consistently make good choices on their own behalf, the problem will not be solved.

Information cards have several key advantages over username/password credentials:

- **No weak, reused, lost, forgotten or stolen credentials:** Because no password is typed in or sent, passwords cannot be stolen or forgotten.
- **Better site authentication; less phishing:** Because authentication can be based on unique keys generated for every information card/site pair, the keys known by one site are useless for authentication purposes at another, even for the same information card. This directly addresses the phishing and fake website problems.
- **Data Minimization:** Because information cards can re-supply identity information or claim values (e.g., name, address, and e-mail address) to other sites with whom they are dealing, those sites don't need to store this data between sessions. Retaining less data, or data minimization, means that sites have fewer vulnerabilities. (See Law 2.)
- **Consistent Interface = Better choices:** Programs like Cardspace implement a standard user interface for working with digital identities. Perhaps the most important part of this interface, the screen used to select an identity to present to a site, is shown in the Figure above.

There are many information card systems. It is worth noting that, by extending the "real-world" visual metaphors and cues of the wallet containing various cards and credentials, information card software such as that by Microsoft makes it possible for users to be in better control of their digital identities. We encourage interested readers to read the seminal whitepapers freely available at **www.identityblog.com** which further explain and clarify the Laws of Identity and information cards in greater detail.

Let us now turn to the privacy features embedded in the identity metasystem.

PRIVACY ANALYSIS AND COMMENTARY ON THE 7 LAWS OF IDENTITY

In light of the preceding discussion and the identity challenges and opportunities that lie ahead, we carried out the following privacy analysis and commentary on the 7 Laws of Identity (and, by extension, on the identity metasystem that those laws collectively describe).

The following chart is the summary result of our efforts to "map" fair information practices to the Laws of Identity, in order to explicitly extract their privacy-protective features. The result is a commentary on the Laws that "teases-out" their privacy implications, for all to consider.

In brief, the privacy-embedded Laws of Identity, when implemented, offer individuals:

- easier and more direct user control over their personal information when online;
- enhanced user ability to minimize the amount of identifying data revealed online;
- enhanced user ability to minimize the linkage between different identities and actions;
- enhanced user ability to detect fraudulent messages and web sites, thereby minimizing the incidence of phishing and pharming.

The 7 Laws of Identity	7 Privacy-Embedded Laws of Identity
LAW #1: USER CONTROL AND CONSENT	**LAW #1:** PERSONAL CONTROL AND CONSENT
Technical identity systems must only reveal information identifying a user with the user's consent.	Technical identity systems must only reveal information identifying a user with the user's consent. Personal control is fundamental to privacy, as is freedom of choice. Consent is pivotal to both. *Consent must be invoked in the collection, use and disclosure of one's personal information. Consent must be informed and uncoerced, and may be revoked at a later date.*
LAW #2: MINIMAL DISCLOSURE FOR A CONSTRAINED USE	**LAW #2:** MINIMAL DISCLOSURE FOR LIMITED USE: DATA MINIMIZATION
The identity metasystem must disclose the least identifying information possible, as this is the most stable, long-term solution.	The identity metasystem must disclose the least identifying information possible, as this is the most stable, long-term solution. It is also the most privacy protective solution. *The concept of placing limitations on the collection, use and disclosure of personal information is at the heart of privacy protection. To achieve these objectives, one must first specify the purpose of the collection and then limit one's use of the information to that purpose. These limitations also restrict disclosure to the primary purpose specified, avoiding disclosure for secondary uses. The concept of data minimization bears directly upon these issues, namely, minimizing the collection of personal information in the first instance, thus avoiding the possibility of subsequent misuse through unauthorized secondary uses.*
LAW #3: JUSTIFIABLE PARTIES	**LAW #3:** JUSTIFIABLE PARTIES: "NEED TO KNOW" ACCESS
Identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.	Identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship. This is consistent with placing limitations on the disclosure of personal information, and only allowing access on a "need-to-know" basis. *Only those parties authorized to access the data, because they are justifiably required to do so, are granted access.*

The 7 Laws of Identity	7 Privacy-Embedded Laws of Identity
LAW #4: DIRECTED IDENTITY	**LAW #4:** DIRECTED IDENTITY: PROTECTION AND ACCOUNTABILITY
A universal identity metasystem must support both "omnidirectional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.	A universal identity metasystem must be capable of supporting a range of identifiers with varying degrees of observability and privacy. Unidirectional identifiers are used by the user exclusively for the other party, and support an individual's right to minimize data linkage across different sites. This is consistent with privacy principles that place limitations on the use and disclosure of one's personal information. At the same time, users must also be able make use of omnidirectional identifiers provided by public entities in order to confirm who they are dealing with online and, thereby ensure that that their personal information is being disclosed appropriately. To further promote openness and accountability in business practices, other types of identifiers may be necessary to allow for appropriate oversight through the creation of audit trails.
LAW #5: PLURALISM OF OPERATORS AND TECHNOLOGIES	**LAW #5:** PLURALISM OF OPERATORS AND TECHNOLOGIES: MINIMIZING SURVEILLANCE
A universal identity solution must utilize and enable the interoperation of multiple identity technologies run by multiple identity providers.	The interoperability of different identity technologies and their providers must be enabled by a universal identity metasystem. Both the interoperability *and* segregation of identity technologies may offer users more choices and control over the means of identification across different contexts. In turn, this may minimize unwanted tracking and profiling of personal information obtained through surveillance of visits across various sites.
LAW #6: HUMAN INTEGRATION	**LAW #6:** THE HUMAN FACE: UNDERSTANDING IS KEY
The identity metasystem must define the human user to be a component of the distributed system, integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.	Users must figure prominently in any system, integrated through clear human-machine communications, offering strong protection against identity attacks. This will advance user control, but only if users truly understand. Thus, plain language in all communications used to interface with individuals is key to understanding. Trust is predicated on such understanding.
LAW #7: CONSISTENT EXPERIENCE ACROSS CONTEXTS	**LAW #7:** CONSISTENT EXPERIENCE ACROSS CONTEXTS: ENHANCED USER EMPOWERMENT AND CONTROL
The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.	The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies. We return full circle to the concept of individual empowerment and informed consent. Clear interfaces, controls and options that enhance an individual's ability to exercise control across multiple contexts in a reliable, consistent manner will serve to enhance the principle of informed consent.

CONCLUSIONS

The Internet was built without a way to know who and what individuals are communicating with. This limits what people can do and exposes computer users to potential fraud. If nothing is done, the result will be rapidly proliferating episodes of theft and deception that will cumulatively erode public trust. That confidence is already eroding as a result of spam, phishing, pharming and identity theft, which leaves online consumers vulnerable to the misuse of their personal information and minimizes the future potential of e-commerce. The privacy-embedded 7 Laws of Identity supports the global initiative to empower consumers to manage their own digital identities and personal information in a much more secure, verifiable and private manner.

Identity systems that are consistent with the privacy-embedded 7 Laws of Identity will help consumers verify the identity of legitimate organizations before they decide to continue with an online transaction. Consumers today are being spammed, phished, pharmed, hacked and otherwise defrauded out of their personal information in alarming numbers, in large part because there are few reliable ways for them to distinguish the "good guys" from the "bad."

E-commerce providers are taking note of this trend because declining consumer confidence and trust are especially bad for business. The next generation of intelligent and interactive web services ("Web 2.0") will require more, not fewer, verifiable identity credentials, and much greater mutual trust in order to succeed.

Just as the Internet emerged from connecting different proprietary networks, an "Identity Big Bang" is expected to happen once an open, non-proprietary and universal method to connect identity systems and ensure user privacy is developed, in accordance with universal privacy principles. Already, there is a long and growing list of companies and individuals that endorse the 7 Laws of Identity and are working towards developing identity systems that conform to them. Participants include e-commerce sites, financial institutions, governments, Internet service providers, mobile telephony operators, certificate authorities, and software vendors for a broad range of platforms.

Our efforts to describe the 7 privacy-embedded Laws of Identity are intended to inject privacy considerations into discussions involving identity – specifically, into the emerging technologies that will define an interoperable identity system. We hope that our commentary will stimulate broader discussion across the Internet blogosphere and among the "identerati."

We also hope that software developers, the privacy community and public policymakers will consider the 7 privacy-embedded Laws of Identity closely, discuss them publicly, and take them to heart. Promoting privacy-enhanced identity solutions at a critical time in the development of the Internet and e-commerce will enable both privacy and identity to be more strongly protected.

APPENDIX A: **FAIR INFORMATION PRACTICES**

CSA PRIVACY CODE

Principles in Summary

Ten interrelated principles form the basis of the CSA Model Code for the Protection of Personal Information. Each principle must be read in conjunction with the accompanying commentary.

1. **Accountability:** An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
2. **Identifying Purposes:** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
3. **Consent:** The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
4. **Limiting Collection:** The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. **Limiting Use, Disclosure, and Retention:** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.
6. **Accuracy:** Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
7. **Safeguards:** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
8. **Openness:** An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
9. **Individual Access:** Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. **Challenging Compliance:** An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Source: **www.csa.ca/standards/privacy**

APPENDIX B: INFORMATION SOURCES AND OTHER USEFUL READING MATERIALS

The Case for Privacy-Embedded Laws of Identity in the Digital Age
Identity Theft Revisited: Security is Not Enough
www.ipc.on.ca

Kim Cameron's Identity Weblog
www.identityblog.com

The LAWS OF IDENTITY
An introduction to Digital Identity - the missing layer of the Internet.
www.identityblog.com/?page_id=354

The IDENTITY METASYSTEM
A proposal for building an identity layer for the Internet
www.identityblog.com/?page_id=355

IDENTITY MANAGEMENT RESEARCH & DEVELOPMENT PROJECTS

- InfoCard / CardSpace: **www.identityblog.com/wp-content/resources/design_rationale.pdf**
- Open Source identity Selector (OSIS) project: **http://osis.netmesh.org**
- Shibboleth: **http://shibboleth.internet2.edu/about.html**
- Eclipse Higgins: **www.eclipse.org/higgins/** & **http://spwiki.editme.com/HigginsInTheNews**
- Bandit: **http://forgeftp.novell.com//bandit/Bandit_f.pdf** & **www.bandit-project.org**
- Yadis: **http://yadis.org** & **www.openidenabled.com**
- OpenID: **www.openid.net** & **www.openidenabled.com**
- Private Credentials: **www.credentica.com**
- Liberty Alliance Project: **www.projectliberty.org**

IDENTITY MANAGEMENT RESEARCH

- EU Future of Identity in the Information Society (FIDIS): **www.fidis.net**
- EU Privacy and Identity Management for Europe (PRIME): **www.prime-project.eu**

SELECT ANALYST AND MEDIA INFORMATION SOURCES

- Federal Financial Institutions Examination Council, *Authentication in an Internet Banking Environment*, October 2005: Guidance document at: **www.ffiec.gov/pdf/authentication_guidance.pdf**
- National Consumers League, *A Call for Action: Report from the NCL Anti-Phishing Retreat*, March 2006: Press Release at: **www.nclnet.org/news/2006/Phishing_Report_03162006.htm**
- *Gartner Survey Shows Frequent Data Security Lapses and Increased Cyber Attacks Damage Consumer Trust in Online Commerce*, June 2005 at **www.gartner.com/press_releases/asset_129754_11.html**

CONTACT

General inquiries should be directed to:

Tel: (416) 326-3333
1-800-387-0073
Fax: (416) 325-9195
TTY (Teletypewriter): (416) 325-7539
e-mail: info@ipc.on.ca
Website: www. ipc.on.ca

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

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