

**Commissioner's Presentation to October 18th Press Conference at the Westin
Harbour Castle Hotel on the white paper, *7 Laws of Identity: The Case for
Privacy-Embedded Laws of Identity in the Digital Age***

Good morning Ladies and Gentlemen,

I want to add my thanks to each of you for coming out today. I am going to talk about an issue that ultimately could affect every single person who ventures onto the Internet.

With the exponential growth of online fraud – phishing, pharming, identity theft the existing identity infrastructure of the Internet is no longer sustainable. Deceptive online practices are threatening to cripple e-commerce. Consumer confidence and trust are at an all-time low, and once people lose faith in any type of system they interact with, they either stop using it or curtail their use substantially.

After citing some of the current problems, I'm going to unveil an ambitious plan to address these problems by building privacy right into the architecture of the next generation of the Internet.

So, let's start with: what is the underlying problem?

It has many symptoms, and has been described in various ways, including:

- the growing disconnect between the real and online worlds;
- rampant online digital fraud, through spoofing, phishing or spyware;
- the rapid increase in identity theft, fueled by the widespread availability and (mis)use of personally identifiable information;
- Password Fatigue: (I know you've all experienced it) people either forget their passwords, or choose easy-to-guess passwords that others can readily discover.

These various problems can be collapsed into three general ones:

No. 1: **Online fraud and security concerns** are inhibiting user confidence, trust and threatening the growth of e-commerce services. Think of spam, phishing, pharming, spyware, etc. On the Internet, there is simply no consistent way of authenticating identity, and thus fraud abounds.

No. 2: Fears of **online surveillance** and the excessive collection, use and disclosure of personal information are also diminishing confidence and use in the Internet. Think of Internet search records, e-mail messages and web postings, cell

phone records, IP addresses, and SIN/SSNs. Once collected, sooner or later, the identifying data will be used by someone else, for secondary purposes that the user is most likely unaware of.

No. 3: **General Lack of user empowerment and control** online over one's own personal data is also diminishing confidence. Many users are simply unable to detect spoofing and phishing attacks. And they are burdened with more and more assigned username/password credentials that they must remember and use securely. It's just too much to expect of users. Therefore, their ability to make informed decisions online is being steadily diminished.

All of these privacy problems are problems of IDENTITY:

- users aren't able to confirm others' identities – as in various websites they deal with;
- users can't minimize the collection, use and disclosure of their own digital identity information by others, nor can they control their online identity relationships;

These identity and privacy issues are holding back the full potential of the Internet.

So, what's the solution?

ENTER the 7 LAWS of IDENTITY and the creation of an IDENTITY METASYSTEM

I believe there is a way to protect privacy and to promote enhanced user control in tomorrow's world of next-generation networked services, dubbed "Web 2.0."

What we need is a fresh new vision and direction, on a grand systemic scale, to confront diminished confidence and trust head-on, AND to ensure that the Internet does not become a medium for surveillance and privacy invasion.

Enter the *7 Laws of Identity*. These are a set of far-reaching technology design principles that will guide the emergence of a universal, interoperable system of digital identities.

This was spearheaded by Microsoft and its Chief Identity Architect, Kim Cameron. The *7 Laws* were developed through open dialogue by experts from all around the world.

And, most notably, the *7 Laws* are completely non-proprietary and free for all to adopt. They are being endorsed and adopted by virtually all the major technology players.

Make no mistake: this is the NEXT WAVE. Identity is the future of privacy. The time to start building privacy in to it is NOW – We don't have a minute to spare.

THE REAL CHALLENGE IS BUILDING PRIVACY INTO THE ARCHITECTURE ITSELF

Great care must be taken that an interoperable identity system does not become an infrastructure of universal surveillance – this could just as easily be the outcome as a privacy-protective system.

But the beauty of the *7 Laws* is that privacy is interwoven throughout each Law, and when the *Laws* are applied, exciting new privacy options will become possible.

In my view, the *7 Laws of Identity* offer immense potential to enhance personal control over the privacy and security of one's personal data online, while also empowering users to have confidence in their online transactions.

I've always held the view that privacy must be built into the design and development of all new technologies. Consistent with that, we have produced a paper that describes some of the ways that privacy may be applied to the *7 Laws*, enhancing its privacy protective features.

This paper is, in fact, the result of our "mapping" privacy principles into the *7 Laws*.

The result, the *Privacy-Embedded Laws of Identity*, is a commentary on the *Laws* that "teases-out" their privacy implications, for all to consider, in an effort to ensure that the promise, in fact, becomes a reality.

We were guided by the idea that people should have the same range of privacy options and control online, as they do offline.

So, for example, in the physical world it would be pretty easy for you to spot a fake branch of your bank, but online, spoofing tricks thousands upon thousands of people – and it is a trivial exercise to do so.

In the real world, you can show an ID card to a store clerk to prove your identity, authorization or eligibility (e.g. age discount), leaving no traces behind, but in the online world, detailed records are collected and kept, perhaps forever.

Finally, in the real world, you can easily manage your identities in your wallet, by choosing to display the appropriate identity card (coffee club card, library card, passport, driver's licence) according to specific contexts. But in the online world, there is no convenient way to manage our various identities in a parallel manner, and to keep our online activities from being merged together to form profiles about us.

Why can't we enjoy the same privacy rights and expectations online as offline??

Fortunately, by applying the 7 Laws of Identity, we will be able to.

Let's use a concrete, specific example to illustrate how. Behind me is a screen snapshot of a computer program that runs on your PC, called CardSpace. CardSpace functions like a virtual wallet.

Microsoft is among the first to develop a user client application, called Cardspace, in compliance with the Laws and which enable the adoption of *Information Cards*.

In this wallet are *Information Cards* – tokens that represent your different identities and contain the various credentials that identify you to other parties online. When released with Vista OS, users will be able to present their Information Cards online just as they do offline, with security and confidence that they cannot be stolen. (Give examples of a “contact info” card and a “Visa” payment card.

The benefits of programs like CardSpace (BTW other companies are developing similar open-source user interfaces for Information Cards for Macs, Linux, cell phones, PDAs, etc) are as follows:

Defeats phishing and online fraud, security risks – by enabling users to detect spoofing, and take appropriate (non) action, such as not providing sensitive banking information or passwords. At a fraudulent site, the Information Card simply will not work.

Minimize disclosure of personal information online – enables users to present the *minimum* personal information necessary to support a given transaction, like proving age for discounts and eligibility for access to resources – without any need to reveal your full identity.

User Empowerment and Control – enables users to manage and control their various identities online in the same manner that they do offline. The personal

information can be entirely stored locally on the users' machine instead of in big centralized databanks operated by third parties. By being able to manage many different online identities, users can keep their various identities and activities separated, and defeat surveillance.

I'm going to turn it over to Peter Cullen and Kim Cameron now, after which I will have a concluding comment, and I will be happy to take your questions.

IMPLICATIONS FOR INDIVIDUAL USERS

The Privacy-Embedded 7 Laws of Identity offer:

- Easier and more direct control over one's personal information when online;
- Embedded ability to minimize the amount of identifying data revealed online;
- Embedded ability to minimize the linkage between different identities and online activities;
- Embedded ability to detect fraudulent email messages and web sites (less spam, phishing, pharming, online fraud).