Commissioner Ann Cavoukian unveils plan
for privacy-embedded Internet identity

TORONTO – 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" online.

Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario, today announced her support for a global online identity system framework by outlining seven far-reaching "privacy-embedded" laws, which would help consumers verify the identity of legitimate organizations before making online transactions.

These laws were inspired by the 7 Laws of Identity formulated through a global dialogue among security and privacy experts, headed by Kim Cameron, Chief Identity Architect at Microsoft. The 7 Laws of Identity propose the creation of a revolutionary "identity layer" for the Internet, providing a broad conceptual framework for a universal, interoperable identity system.

Dr. Cavoukian's *7 Laws of Identity*: *The Case for Privacy-Embedded Laws of Identity in the Digital Age* incorporates additional key insights from the privacy arena. An extension of the original 7 Laws, they encourage privacy-enhanced features to be embedded into the design of the IT architecture and be made available early in the emerging universal identity system.

The Internet was built without a way to know who and what individuals are connecting to. This limits what people can do and exposes computer users to potential fraud. If the IT industry and government do nothing, 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 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 Laws of Identity* support the global initiative to empower consumers to manage their own digital identities and personal information in a much more secure, verifiable and private manner.

"Just as the Internet saw explosive growth as it sprang from the connection of 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 privacy principles," said Dr. Cavoukian. "Microsoft started a global privacy momentum. Already, there is a long and growing list of companies and individuals who now endorse the 7 Laws of Identity and are working towards developing identity systems that conform to them."

 "We are honoured to work with Dr. Cavoukian on this project, who along with us and other IT companies are endorsing global privacy laws and fair information practices," said Peter Cullen, Chief Privacy Strategist, Microsoft. "Best business practices that ensure both security and

identity are what is needed to help keep the Internet's integrity intact. These 7 Laws, with specific articulation of privacy protections, are a big step in that direction."

Other privacy-enhanced laws will help to minimize the risk that one's online identities and activities will be linked together, said Dr. Cavoukian. "We already expect this in the real world when we present a library card, for example, to check out a book, and present our passport to cross a national border. We don't expect these to be linked together. Nor is the access card we use to enter our office the same as the transit pass we use to board a bus. In the physical world, different transactions require different identity credentials, but they need not be linked together. It should be no different in the online environment."

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 to succeed.

Identity systems that are consistent with the *Privacy-Embedded Laws of Identity* will help consumers verify the identity of legitimate organizations before they decide to continue with an online transaction.

These *Privacy-Embedded Laws* 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 websites, thereby minimizing the incidence of phishing and pharming.

Corresponding *Privacy-Embedded* Principles

Take, for example, Law #1, *Personal Control and Consent,* which emphasizes that individuals should be in full local control of their own identity information, and exercise informed consent over how their identity information is collected and used by others. One privacy benefit of applying this principle is that identity credentials could be stored locally and securely on a user's own computer rather than in a centralized online database.

Another example: Law #2, *Minimal Disclosure for Limited Use: Data Minimization*, speaks to building technical identity systems that minimize the amount of identity information used and disclosed in a given online transaction. In the privacy world, a cardinal rule is that the identification provided should be proportional to the sensitivity of the transaction and its purpose. Why should a credit card number ever be used to verify one's age? Put another way, why isn't there a credential that allows people to prove they're over 65 without revealing **all** of their other identity information? If someone can prove she is a bona fide university student to gain preferential access to online resources at other educational institutions, then why is her name needed? These privacy-enhanced solutions are all possible under the *Privacy-Embedded Laws of Identity.*

"We call upon software developers, the privacy community and public policymakers to consider the *Privacy-Embedded Laws of Identity* closely, to discuss them publicly, and take them to heart," Dr. Cavoukian declared. "In joining with us to promote privacy-enhanced identity solutions at a critical time in the development of the Internet and e-commerce, both privacy and identity/security will more likely be strongly protected."

The Information and Privacy Commissioner is appointed by and reports to the Ontario Legislative Assembly and is independent of the government of the day. The Commissioner's mandate includes overseeing the access and privacy provisions of the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act*, as well as the *Personal Health Information Protection Act*, and helping to educate the public about access and privacy issues.

Media Contacts:

Bob Spence
Communications Co-ordinator
Direct line: 416-326-3939
Cell phone: 416-873-9746
Toll free: 1-800-387-0073
bob.spence@ipc.on.ca
www.ipc.on.ca

Tiffany Baggetta
Direct   line: 905-278-5500,   x225
Cell: 905-464-7057
Toll free: 1-877-363-6466
tiffany.baggetta@ipc.on.ca

Additional Resources:

7 Laws of Identity: *The Case for Privacy-Embedded Laws of Identity in the Digital Age*
www.ipc.on.ca

Kim Cameron's Identity Weblog
www.identityblog.com/

The LAWS OF IDENTITY
The key to this site: 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