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

INTRODUCTION

This work 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.

We believe that the "7 Laws" (a.k.a. "technologically-necessary principles of identity management") will profoundly shape the architecture and growth of a universal, interoperable identity system needed to enable the Internet to evolve to the next level of trust and capability.

A universal identity system will have profound impacts on privacy since the digital identities of people * and the devices associated with them * constitute personal information. Great care must be taken that an interoperable identity system does not become an infrastructure of universal surveillance.

This document is the result of "mapping" privacy fair information practices over the 7 Laws of Identity to 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.

We believe that privacy is woven throughout 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 - its development must be fostered and encouraged.

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

1

USER CONTROL AND CONSENT

Technical identity systems must only reveal information identifying a user with the user's consent.

PERSONAL CONTROL AND 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.

2 MINIMAL DISCLOSURE FOR A CONSTRAINED USE

The identity metasystem must disclose the least identifying information possible, as this is the most stable, long-term solution.

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. 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.

3

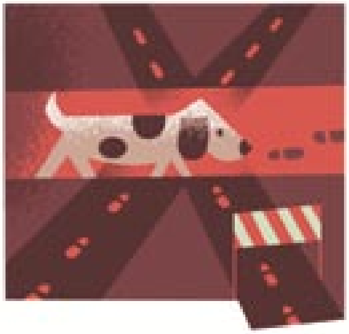
JUSTIFIABLE PARTIES

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.

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. 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.



4

DIRECTED IDENTITY

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.

DIRECTED IDENTITY: PROTECTION AND ACCOUNTABILITY

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.

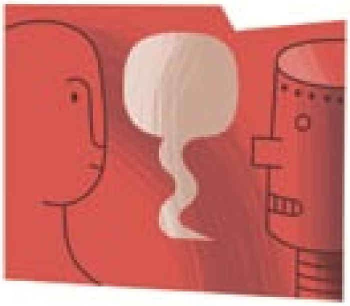
5

PLURALISM OF OPERATORS AND TECHNOLOGIES

A universal identity solution must utilize and enable the interoperation of multiple identity technologies run by multiple identity providers.

PLURALISM OF OPERATORS AND TECHNOLOGIES: MINIMIZING SURVEILLANCE

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.



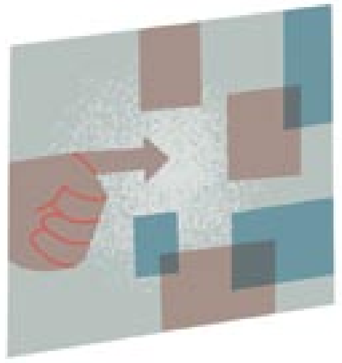
6

HUMAN INTEGRATION

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.

THE HUMAN FACE: UNDERSTANDING IS KEY

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.



7

CONSISTENT EXPERIENCE ACROSS CONTEXTS

The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

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. 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.

FOR MORE INFORMATION

The Case for Privacy-Embedded Laws of Identity in the Digital Age

www.ipc.on.ca (http://www.ipc.on.ca/)

Kim Cameron's Identity Weblog

www.identityblog.com (http://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

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