The Case for Privacy-Embedded Laws of Identity

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario

International Association of Privacy Professionals

2006 IAPP Privacy Academy

October 19, 2006

IPC

Presentation Outline

1. *Setting the Stage*
2. *Phishing, Pharming, Vishing*
3. *Possible Solutions*
4. *The “Big” Idea*
5. *The 7 Laws of Identity*
6. *Privacy-Embedded 7 laws*
7. *Conclusion*

IPC

Setting the Stage

IPC

Setting the Stage

- With the exponential growth of online fraud, the existing identity infrastructure of the Internet is no longer sustainable;
- Online fraud is growing at an alarming rate and threatening to cripple e-commerce;
- Consumer fears and expectations are on the rise, while confidence and trust are dropping.

IPC

Phishing, Pharming, Vishing

IPC

Phishing, Pharming and Vishing

- Fraudulent online capture and misuse use of personal information;
- Significant economic consequences – a root cause of identity theft and other deceptive practices;
- How can individuals be certain of the identity of companies online – ***are they real?***
- Companies' reputations and brands are impacted by deceptive online practices.

IPC

Phishing, Pharming, and Vishing (Cont'd)

- Phishing is like spam but more sophisticated – it's targeted and malicious;
- A criminal activity, phishing is perceived as an invasion of privacy;
- Phishing may involve installing spyware on individuals' computers;
- The phishing problem is skyrocketing and, ***no one is immune;***
- Pharming is technological exploitation that tricks users into visiting a fraudulent website;
- Vishing is a variant of phishing that uses VoIP.

IPC

Identity and Privacy Crisis

Growing identification requirements pose privacy problems:

- **Online fraud and security concerns** are inhibiting confidence, trust, and the growth of e-commerce;
- **Fears of online surveillance** and excessive collection, use and disclosure of identity information by others are also diminishing confidence and use in the Internet;
- **Lack of individual user empowerment and control** online over one's own personal data is diminishing confidence and use in the internet;
- **Password fatigue:** weak, reused passwords;

- **What is Needed:** improved user control, data minimization techniques, privacy protection, and stronger security.

IPC

Possible Solutions

IPC

Possible Solutions

Education, Authentication and Security

- Solutions are complex – education is necessary but insufficient;
- Consumer technologies should be secure by design – strong privacy and data protection should be the default setting in all browsers, software, computers, etc;
- Improved methods of site and user authentication should be adopted.

IPC

The "Big" Idea

IPC

A Single Identity Metasystem

- Before the Internet, there were many different networks that did not speak the same language;
- With the introduction of TCP/IP, thousands of network externalities bloomed, and the Internet exploded;
- A similar phenomenon is being predicted today: a “TCP/IP” for linking different identity systems will open up endless new e-commerce possibilities ***– enter the Identity Metasystem, based on the 7 Laws of Identity.***

IPC

The Genius of the Identity Metasystem

- Developed by Microsoft's Chief Identity Architect, Kim Cameron, the 7 Laws of Identity are technologically-necessary principles of identity management;
- The 7 Laws describe an identity metasystem for allowing different identity systems to function simultaneously;
- The genius of the identity metasystem is that it seeks to allow interoperability, with minimal disruption or modification to current ID systems.

IPC

The Big Bang

Supporters of the 7 Laws and the Identity Metasystem call this the “Identity Big Bang” that will enable ubiquitous intelligent services and a true marketplace for portable identities ***(Web 2.0).***

IPC

The 7 Laws of Identity

IPC

The Attributes of the 7 Laws of Identity

- A set of architectural “meta-standard” design principles to promote interoperability between digital identity systems;
- Developed by open, international consensus-building among wide range of stakeholders. The 7 Laws are complementary and non-proprietary;
- Increases users’ ability to authenticate online sites, combat phishing, defeat spoofing fears.

IPC

The Attributes of the 7 Laws of Identity (Cont'd)

- Empowers users to manage their own digital identities and personal information online;
- The seven laws are truly privacy-enabling: they make possible the development and emergence of privacy-enhancing identity solutions (with some help from the privacy world).

IPC

The Attributes of the 7 Laws of Identity (Cont'd)

- Many of the large technology developers, Internet research consortia players and even critics of Microsoft have already signed on to the concept;
- A universal identity system will have a profound impact on privacy since the digital identities of people, and the devices associated with them, all constitute personal information – they can also pave the way for an infrastructure of surveillance.

IPC

The Attributes of the 7 Laws of Identity (Cont'd)

- Remember, privacy implications flow from connecting our identities to the identities of machines that we own, operate, and carry with us, (computers, cell phones, PDAs, Websites);
- Consider any unique identifier – its fundamental purpose in life is to serve as a basis for data matching and data aggregation, over time;
- This is the exact opposite of a privacy-enhancing practice – it flies in the face of data minimization.

IPC

Building User-Centric Privacy into an Identity Metasystem

- The emergence of an Identity Metasystem is a profound development – there has never been a more strategic time to ensure that privacy interests are built into the new architecture of identity;
- My office has always advocated that privacy be built into the design and operation of information systems and technologies, from the start: ***Privacy by Design;***
- Since we noticed many parallels between the 7 Laws and Fair Information Practices, the two sets of principles being fundamentally complementary, we decided to embed privacy into them.

IPC

Privacy-Embedded

Laws

IPC

IPC's "Privacy-Embedded" 7 Laws of Identity

- An identity metasystem (described by the 7 Laws) is a necessary but not sufficient condition for privacy-enhancing options to be developed.
- What was needed was privacy-enabling design options for identity systems to be identified and then embedded, thus immersing privacy and data protection into the design;
- The privacy-embedded Identity Metasystem is the result of "mapping" fair information practices over the 7 Laws, to explicitly extract their privacy-protective features;
- The result is a commentary on the 7 Laws that extracts its privacy implications, for all to consider.

IPC

“Privacy-Embedded” 7 Laws of Identity

1. **Personal Control and Consent:**

   Technical identity systems must only reveal information identifying a user with the user’s consent;

2. **Minimal Disclosure For Limited Use: Data Minimization**
   The Identity Metasystem must disclose the least identifying information possible. This is the most stable, long-term solution. It is also the most privacy protective solution;

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;

IPC

“Privacy-Embedded” 7 Laws of Identity (Cont’d)

4. **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;

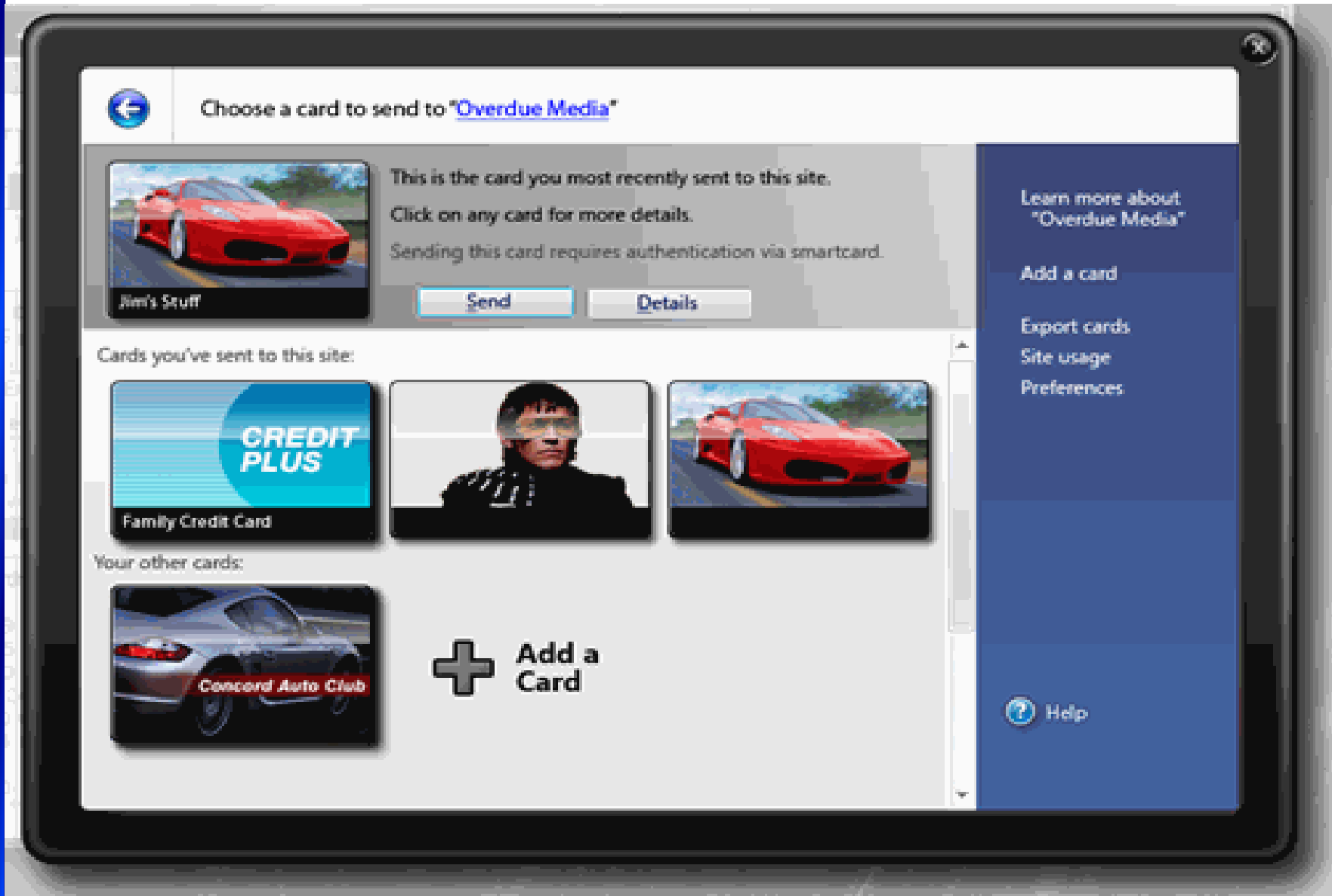
5. **Pluralism of Operators and Technologies: Minimizing Surveillance**
   The interoperability of different identity technologies and their providers must be enabled by a universal Identity Metasystem;

6. **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;

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.

IPC

Information Cards



IPC

Implications for 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).

IPC

Conclusion

- With the exponential growth of online fraud, the existing identity infrastructure of the Internet is no longer sustainable;
- What is needed: a single interoperable Identity Metasystem that is respectful of privacy;
- Consider the vision of the 7 Laws of Identity;
- Consider the “Privacy-Embedded” 7 Laws, which infuse privacy into the development of an Identity Metasystem, in an effort to avoid the emergence of an infrastructure of surveillance;
- Identity will be integrally linked to the future course of privacy – therefore, privacy must be built into the design of existing and future identity systems.

IPC

How to Contact Us

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada

M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

IPC