



“Privacy by Design”

Build it In

Ann Cavoukian, Ph.D.

**Information and Privacy Commissioner
Ontario**

Annual Privacy and Security Conference

Victoria, British Columbia

February 16, 2007



Presentation Outline

- 1. Privacy by Design*
- 2. Identity Management: The Need for an Over-Arching Plan*
- 3. The 7 Laws of Identity*
- 4. “Privacy-Embedded” 7 Laws*
- 5. RFID Privacy Guidelines*
- 6. Biometrics White Paper*
- 7. Conclusion*



Privacy by Design



Privacy by Design

*“Technology knows no borders;
... Technology transcends jurisdiction.”*

- This has been the driving force behind my office’s approach to privacy, in shaping public policy and organizational practices, on a wide range of technology-related issues, including:
- RFIDs, biometrics, smartcards, PKI, DRM, P3P, identity management systems, video surveillance, national ID cards, electronic road toll systems, and Social Networks (Facebook).



“Build It In”

- Build in privacy – up front, into the design specifications into the architecture; if possible embed privacy right into the technology used – *bake it in*;
- Assess the risks to privacy: conduct a privacy impact assessment; follow up with annual privacy audits;
- Data minimization is key: minimize the routine collection and use of personally identifiable information – use encrypted or coded information whenever possible;
- Use privacy enhancing technologies (PETs): give your customers maximum control over their data.



Ontario IPC Involvement With External Organizations

- Guardent Security – Privacy Diagnostic Tool;
- Carnegie-Mellon CyLab – Privacy Interest Group;
- Deloitte & Touche – The Security-Privacy Paradox: Issues, Misconceptions and Strategies;
- Canadian Marketing Association – Incorporating Privacy into Marketing and Customer Relationship Management;
- EPCglobal Canada– Privacy Guidelines for RFID Information Systems;
- IBM Privacy Institute; Privacy Management Council;
- Bank of Montreal – A Portable Privacy Primer;
- Microsoft, IBM, SunMicrosystems, Oracle, Hewlett-Packard, Liberty Alliance.



“U-Prove SDK”

Credentica Privacy Technology Product

- **Founder and CEO of Credentica, Dr. Stefan Brands** has developed a privacy-enhanced user-centric identity management tool that can be integrated with current identity management systems, and is thoroughly consistent with the privacy-embedded 7 Laws of Identity, notably:
 - Personal Control and Consent;
 - Minimal Disclosure for Limited Use: Data Minimization;
 - Justifiable Parties: Need to Know Access;
 - Directed Identity: Protection and Accountability, and;
 - Pluralism of Operators and Technologies: Minimizing Surveillance.
- This is a true Privacy Enhancing Technology (PET) – one which has been tested and vetted extensively by over a dozen world-class cryptographers and leading companies.



***Identity Management:
The Need for an
Over-Arching Plan***



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.*



The Vision of the Identity Metasystem

- Developed by Microsoft's Chief Identity Architect, Kim Cameron, in collaboration with many others, the 7 Laws of Identity form a technologically-necessary set of design principles for 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.



“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*).



Privacy-Embedded



Laws



How We Came to Work with Microsoft

- Introduced to the idea of the 7 Laws of Identity and the Identity Metasystem by Kim Cameron, Microsoft's Chief Identity Architect, who directed this endeavor with a diverse group of experts;
- As Commissioner, I was intrigued but wanted to influence the future course of the 7 Laws in the direction of **privacy**. And in order to do that, the language of privacy had to figure prominently in the Laws – it had to be **built in**; so that's what we did.



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.”

— *7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age.*

www.ipc.on.ca/images/Resources/up-7laws_whitepaper.pdf



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.



“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;



“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.



One Example: *Cardspace and Information Cards*

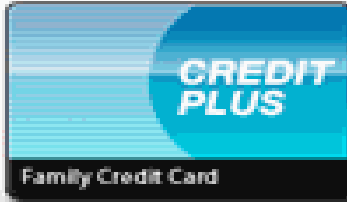
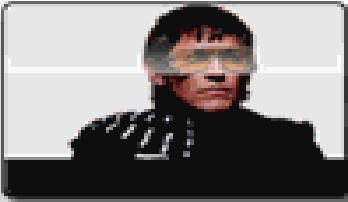
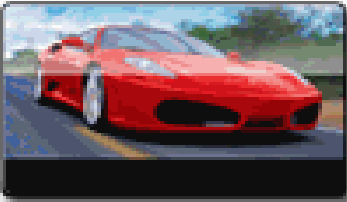
Choose a card to send to ["Overdue Media"](#)

 This is the card you most recently sent to this site.
Click on any card for more details.
Sending this card requires authentication via smartcard.


[Send](#) [Details](#)


Jim's Stuff

Cards you've sent to this site:

-  CREDIT PLUS
Family Credit Card
- 
- 

Your other cards:

-  Concord Auto Club

 Add a Card


Learn more about "Overdue Media"

Add a card

Export cards

Site usage

Preferences

 Help

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 phishing, pharming, online fraud).



Our Ongoing Collaboration on Internet Identity Issues

- October 2006, we called upon software developers, the privacy community and public policy-makers to consider the Privacy-Embedded 7 Laws of Identity closely, to discuss them publicly, and act on them;
- Many have taken us up, stepping forward to present their own ID management projects, and to explain how their solutions are user-centric and privacy-enhancing, resulting in the following two initiatives:



New Initiatives

- IPC is currently in talks with leading members of open-source identity management projects, such as Liberty Alliance and Project Higgins, among others, to pursue opportunities for embedding privacy in online interactions and transactions;
- IBM (w/ Project Higgins) - we are currently exploring the application of privacy-respectful identity-management solutions to identity and authentication transactions where the data subject is not directly involved, but has designated an agent to act on his or her behalf;
- Sun/Oracle/HP (w/Liberty Alliance) - we are currently discussing opportunities to provide privacy analysis and advice on emerging federated identity data-sharing and privacy protocols.



RFIDs



Privacy and RFID Tags

- **Radio Frequency IDentification (RFID)** is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders;
- RFID tags contain information about a product, not an individual (e.g., EPC, size, colour, manufacture date, etc.);

Consumer Reports magazine, June, 2006 cover story:

“The End of Privacy? ...Tiny devices attached to everything you buy could put you under extensive surveillance.”



RFID Privacy Challenges

Perceived lack of transparency and consumer trust:

- RFID technology and current uses not well understood by public; public opinion on RFID still developing;
- Fueled by privacy fundamentalists, many consumers perceive a threat to privacy from possible surveillance or secondary data uses – *even when no threat exists*;
- Lack of consumer voice and input = possibility of a consumer backlash;
- Organizations deploying RFID need to be proactive, *need to take action now*.



IPC and RFIDs

- Spring 2006, the IPC released a DVD discussing RFID tags and privacy: *A Word About RFIDs and your Privacy... in the Retail Sector*;
- Summer 2006, the IPC in collaboration with EPCglobal Canada, issued the publication, *Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines)*, accompanied by a companion piece titled, *Practical Tips for Implementing RFID Privacy Guidelines*;
- 2003 and 2004, other publications that the IPC issued on RFID technology including; *Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology*, and *Guidelines for Using RFID Tags in Ontario Public Libraries*.



RFID Legislative Activity in the United States

- **Two*** states have passed bills that directly address RFID:
 - 2006 – New Hampshire (HB203)
 - 2006 – Wisconsin (AB290)
- An additional **five*** states have passed bills referring to RFID:
 - 2006 – New Hampshire (HB1738)
 - 2006 – Washington (HB2407)
 - 2005 – Wyoming (HB0258)
 - 2005 – California (AB1489)
 - 2002 – New Jersey (S573/S890)
- In 2006, **twenty-six*** bills were introduced dealing with RFID. In 2007, **twelve*** bills have been introduced.

* Estimated



Trends:

U.S. Bills Relating to RFIDs

Since January 2006, bills were introduced on the following issues:

- **Task Forces** (New York, Washington);
- **Consumer Privacy** (Illinois, Missouri, New York, Tennessee, Virginia, Arkansas);
- **Prescription Drug Packaging** (Federal);
- **Human Identification: Microchips in Individuals / Identification Documents / Other Tracking** (New Jersey, Ohio, Michigan, North Dakota, Oklahoma / Alabama, Illinois, Washington, California / Rhode Island, Florida, New Hampshire, California, Washington, Georgia);
- These bills may be advancing through the legislative process, or they may be vetoed or stalled.



Canada

Legislative Landscape

Canadian Privacy Laws:

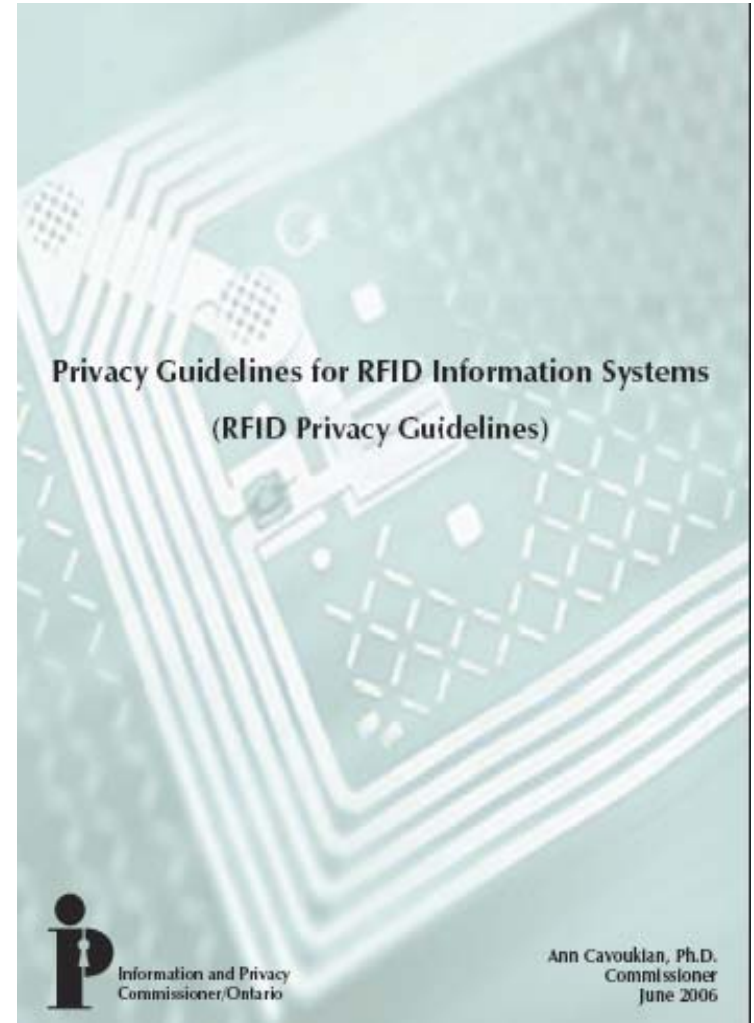
- In Canada, we prefer to pass general-purpose privacy laws, based upon Fair Information Principles, with oversight agencies/authorities;
- Canadian privacy laws are technology-neutral; little specific guidance to IT industry;
- *PIPEDA* is such a law: based upon the 10 principles of the CSA Privacy Code (Schedule 1);
- Emergence of substantially similar provincial privacy laws (AB, BC, QC) and Ontario for health, *PHIPA*.



IPC RFID Privacy Guidelines

- Developed with leading industry standards-setting organization (GS1/EPCglobal Canada);
- Promotes compliance with Canadian privacy laws;
- Strongest, most complete set of RFID guidelines developed to date – promotes compliance with privacy laws and engenders consumer trust.

www.ipc.on.ca/docs/rfidgdlines.pdf





Features of IPC RFID Guidelines

- The *Guidelines* address key privacy issues regarding the use of item-level RFID technology in the retail/commercial sector;
- The purpose of the *Guidelines* is to promote the embedding of privacy laws into RFID technology by addressing concerns about the potential threat to privacy and to build-in the necessary protections for the item-level use of RFID tags by retailers;

The *Guidelines* are based on three principles:

1. Focus on RFID information systems, not technologies;
2. Build in privacy and security from the outset, at the design stage;
3. Maximize individual participation and consent.



Biometrics

White Paper



IPC and Biometrics

- The IPC has been a longstanding proponent of biometric encryption technologies;
- We continue to press for strong privacy protections in the development and deployment of interoperable biometric technologies;
- Active member of the European Biometrics Forum International Biometrics Advisory Council (IBAC).

www.eubiometricforum.com/index.php?option=content&task=view&id=457



European Biometrics Forum

- The European Biometrics Forum (EBF) was launched in 2003; Member of International Biometrics Advisory Council (IBAC);
- Composed of leading biometrics and technology experts, the EBF was established to develop world-class standards, best practices and innovation in the biometrics industry to strengthen trust and confidence in the use of emerging biometric applications;
- The EBF is supported by a network of national biometric organizations, companies, universities and experts across Europe in carrying out research for the development of a roadmap for the European Biometrics industry to 2010.

www.eubiometricforum.com



Biometric Encryption

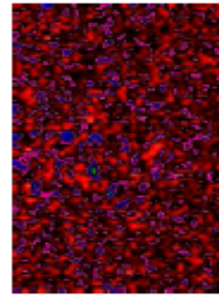
- Biometric encryption is a process that securely binds a PIN or a cryptographic key with a biometric, so that neither the key nor the biometric can be retrieved from the stored template. The key is recreated only if a correct biometric sample (a finger or iris) is presented on verification;
- In biometric encryption, you can use the biometric to encrypt a PIN or a password for numerous applications, such as access to computers or bank machines. The PINs can be 100s of digits in length because you don't need to remember it;
- Most important, the only item that has to be stored in a database is the biometrically encrypted PIN or password, not the biometric template, so privacy is preserved.

IPC Biometrics White Paper



Biometric Encryption:

A Positive-Sum Technology that Achieves Strong
Authentication, Security AND Privacy



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

Alex Stolanov, Ph.D.
Biometrics Scientist

February 2007



IPC Biometrics White Paper (Cont'd)

- The IPC is developing a paper with chief scientist, Alex Stoinov, on the privacy-enhanced uses of biometrics, with a particular focus on the privacy and security advantages of *biometric encryption technology*;
- The paper is intended to engage a broader, non-technical audience in considering the merits of the biometric encryption approach to verifying identity, ensuring strong security, and protecting privacy;
- I introduced the outline of our paper to IBAC at a meeting on December 12, 2006, and received widespread support from the technology companies in attendance;
- This paper was pre-released to IBAC on February 14, 2007, and will be released widely in March,



Conclusion

- Wherever possible, embed privacy into the design of the technology used: *“Privacy by Design.”*
- An entirely new identity metasystem may be needed to combat the steadily growing rates of fraud and deception online;
- Consider the *“Privacy-Embedded” 7 Laws of Identity*;
- RFIDs that have no personal information linked to them pose no threat to privacy;
- For the use of item-level RFIDs in the retail/consumer space, consider our *RFID Privacy Guidelines*;
- The most privacy-protective use of a biometric is one that does not have a template retained in a central database – *consider biometric encryption.*



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