



Functional requirements for privacy enhancing systems

Fred Carter

**Senior Policy & Technology Advisor
Office of the Information & Privacy
Commissioner / Ontario, Canada**

**OECD Workshop on Digital Identity Management
Trondheim, Norway
09 May 2007**

IPC

© Information and Privacy Commissioner of Ontario, 2006



Presentation Outline

- 1. IPC Work*
- 2. Challenge*
- 3. PETs & FIPs*
- 4. IDM: 7 Laws*
- 5. IDM: Biometric Encryption*
- 6. Next Steps*

IPC

© Information and Privacy Commissioner of Ontario, 2006



1. IPC work to date

- Independent agency of gov't; we oversee three laws
- Longstanding interest & involvement in privacy, technology and law/compliance issues.
- IPC approach: constructive engagement; ICT both a threat to and opportunity for privacy; seek pragmatic “win-win” scenarios
- **Some publications:** Path to Anonymity; guidance on use of PKI, DRM, Privacy-embedded 7 Laws of Identity, Biometrics, Biometric Encryption; ID Theft; Intelligent Agents, P3P, RFID, Privacy and the Open Networked Enterprise, Privacy Diagnostic Tool; PIA for health, contactless smart cards; mobile device security; STEPs, etc.
IPC website: www.ipc.on.ca

IPC

© Information and Privacy Commissioner of Ontario, 2006



2. Challenge

- Advent of ICTs, increasingly data-intensive activities, transformed private and public-sector services, many potential benefits
- **Primary challenge: overcoming weak public confidence, trust, use/adoption**
- Relentless negative news, e.g.: multi-million \$\$\$ failures and boondoggles; high-profile privacy & security breaches; poor IT security report cards = loss of confidence in
- **Privacy Can Help**

IPC

© Information and Privacy Commissioner of Ontario, 2006



3. Info Privacy Defined

Effective governance can come from:

1. **Laws, legislation, regulation**
 2. **Industry self-regulation, codes of conduct, best practices, guidelines, standards, policies, audit & certification practices...governance**
 3. **PETs / Technology solutions**
 4. **Public opinion / market acceptance**
- Founded on the Fair Information Practices (FIPs)
 - PETs just one element in the IPC privacy toolkit



© Information and Privacy Commissioner of Ontario, 2005



3. PETs & FIPs

- Many FIPs in use around the world
- FIPs can be condensed into three primary and substantive impulses:
 - 1. Data Minimization
 - 2. User Participation and Control
 - 3. Information Security
- Good success evangelizing to public policymakers, information security, auditors, developers, etc.
- Expressed in myriad ways, depending on context.



© Information and Privacy Commissioner of Ontario, 2005



3. PETs & FIPs

- Building FIPs into ICTs: our Mantra
 - Whole information system, not one component (e.g., RFID tag, smart card, biometric reader)
 - Build privacy in early, at the design stage
 - Privacy/anonymity the default starting point (identifiability, observability, linkability)
 - Maximize involvement and participation of data subjects and system users.
- Identity issues are a subset of information privacy issues



© Information and Privacy Commissioner of Ontario, 2005



4. IDM & 7 Laws

The Case for Privacy-embedded 7 Laws of Identity



© Information and Privacy Commissioner of Ontario, 2005



4. IDM & 7 Laws

Growing online ID req'ts 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

© Information and Privacy Commissioner of Ontario, 2006



4. “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

© Information and Privacy Commissioner of Ontario, 2006



4. “Privacy-Embedded” 7 Laws of Identity

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 and Privacy Commissioner of Ontario, 2006



4. IDM & 7 Laws

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

© Information and Privacy Commissioner of Ontario, 2006



4. IDM & 7 Laws

Attractive Features of the 7 Laws:

- Fresh response/approach to real-world problems
- “Failure” of MS Passport model acknowledged
- Recognition of market drivers for success
- Clear expression of key FIPs, esp. Laws 1 & 2
- If not a PET itself, then an enabling framework/foundation for PETs
- IPC is technology-agnostic w.r.t. how these “Laws” are expressed or obeyed.

IPC

© Information and Privacy Commissioner of Ontario, 2006



4. IDM & 7 Laws

Response to date:

- Neutral to positive reaction from public, policymakers, media, and industry
- Enhanced public awareness and dialogue
- Interest and engagement from other industry and standards initiatives, e.g:
 - Liberty Alliance
 - IBM/Higgins
 - Credentica

IPC

© Information and Privacy Commissioner of Ontario, 2006



5. IDM & Biometric Encryption

The problem:

- Growing biometrics deployment and use poses significant risks and threats to privacy, security
- Biometrics a lifetime permanent identifier, worse than a password (access control)
- Inadequate for large-scale 1:many ID uses.
- Secondary uses, function creep, data matching, surveillance, profiling, discrimination
- Misuse of data: Identity fraud, theft, etc.
- One data breach can trigger public backlash.

IPC

© Information and Privacy Commissioner of Ontario, 2006



5. IDM & Biometric Encryption

BE Embodies core privacy practices:

1. Data minimization: no retention of biometric image or template, minimizing potential for secondary uses, loss, misuse
2. Maximal individual control: Individuals keep their biometric data private, and can use it to generate or change unique (“anonymous”) account identifiers, and encrypt own data.
3. Improved security: authentication, communication and data security are enhanced.

IPC

© Information and Privacy Commissioner of Ontario, 2006



5. IDM & Biometric Encryption

IPC Objectives:

- Stimulate demand for PETs: Bring this biometric technology to attention of public, privacy advocates, policymakers: it is possible and should be considered, even demanded.
- Stimulate supply of PETs: Encourage research, development and marketization of privacy-enhancing technologies as viable solutions for real-world problems.

IPC

© Information and Privacy Commissioner of Ontario, 2006



6. Next Steps

Key stakeholders: (demand-side)

- Public / Media
- Public policymakers
- Privacy advocates

Key stakeholders: (supply-side)

- Industry
- Technologists, Developers
- Integrators

IPC

© Information and Privacy Commissioner of Ontario, 2006



6. Next Steps

Challenge: Increase demand for PETs

- Increase awareness and interest in PETs
- Spotlight, recognize, promote PETs solutions
- Encourage and recognize early adopters, success

Challenge: Increase supply of PETs

- Increase awareness and interest in PETs
- Spotlight, recognize, promote PETs solutions
- Encourage and recognize early adopters, success



© Information and Privacy Commissioner of Ontario, 2006



How to Contact Us

Fred Carter

Senior Policy & Technology Advisor

Information & Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada M4W 1A8

Phone: +1.416.326.3333

Web: www.ipc.on.ca



© Information and Privacy Commissioner of Ontario, 2006



Extra Slides

IPC

© Information and Privacy Commissioner of Ontario, 2006



OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Eight Principles:

1. Collection Limitation
2. Data Quality
3. Purpose Specification
4. Use Limitation
5. Security Safeguards
6. Openness
7. Individual Participation
8. Accountability

IPC

© Information and Privacy Commissioner of Ontario, 2006



Fair Information Practices (CSA Privacy Code)

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure, Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance



IPC

© Information and Privacy Commissioner of Ontario, 2005



PETs & IDM

- Privacy Enhancing Technologies (or Tools) include those that empower individuals to manage their own identities in a privacy enhancing manner.
- These include tools or systems to:
 - anonymize and pseudonymize identities;
 - securely manage login ids and passwords and other authentication requirements;
 - manage contactability or “reachability;”
 - generally, allow users to selectively disclose their PII to others and to exert maximum control over their PII once disclosed.
- Identity issues are a subset of information privacy issues.

IPC

© Information and Privacy Commissioner of Ontario, 2005