Berkman | The Berkman Center for Internet & Society at Harvard Law School

Stanford Law School's
Center for Internet and Society

Bridging OECD Data Protection Principles and The New Identity Management Infrastructure

Mary Rundle
mrundle[at]cyber.law.harvard.edu

OECD-Norway Workshop on Digital Identity Management
Trondheim, Norway – 8 and 9 May 2007

To Cover

- Promise of New IDM Technologies
- Data Protection Principles
- Challenge
- Proposed Solution
- OECD Role?

Promise of New IDM Technologies

Touted benefits:

- Reduce phraud, phishing, pharming, spam
- Provide convenience by eliminating forms
- Avoid the hassle and potential loss of passwords
- Enable automated web services

Promise of New IDM Technologies

Second Internet boom?

Promise of New IDM Technologies

= Enormous personal data flow

Data Protection Principles

How will data protection standards be followed?

For example…

Data Protection Principles

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

Problem:

If data protection principles are binding in some jurisdictions,
will there be a clash from start?

Challenge:

Bridge
data protection principles and
identity management technologies.

Proposed Solution:

Elements –

- Observes international data protection standards;
- Is clear and easy for people;
- Hooks into the identity management infrastructure; and
- Allows audits of how data is treated.
- Affords a mechanism for redress.

Proposed Solution:

Element 1 –
Observes international data protection principles

Point of reference here (+ others) =

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)

Proposed Solution:

Element 2 –
Is clear and easy for people

Creative Commons-like icons

- Human readable
- Lawyer readable
- Machine readable (globally)

	You agree not to use this data for marketing purposes.
	You agree not to trade or sell this data.
	You agree to submit to a third-party audit program on data use; if government has requested access to my data, you agree to involve my governmental ombudsman.
	You agree to make available to me the data that you have on me without my having to pay for it/at a minimal charge.
	You allow me to address inaccuracies in the data and request its removal.
	You agree to take reasonable steps to keep my data secure.
	You agree to bring any disputes we have over your treatment of this data to the Arbitration and Mediation Mechanism of [Organization].

Proposed Solution:

Element 2 –
Is clear and easy for people

Advantages

- Bridges jurisdictional requirements.
- Offers simple choices.
- Allows multiple combinations according to context.
- Works internationally (linguistically).

Proposed Solution:

Element 3 –
Hooks into the identity management infrastructure

- Where policies expressed (e.g., on outside and inside of token)
- How approach can be interoperable
- How negotiations can take place
- How users can have strength in numbers
- Etc.

Proposed Solution:

Element 4 –
Allows audits of how data is treated

- Checks against improper treatment by private actors having access to data.
- Checks against improper treatment by governmental actors having access to data.

Proposed Solution:

Element 4 –
Allows audits of how data is treated

Auditing of private actors' activities

The Bandit Project, led by Novell

- Fully open source and developed in public.
- For more info, see http://www.bandit-project.org.

Proposed Solution:

Element 4 –
Allows audits of how data is treated

Auditing of governments' activities

Government may need access to data, e.g., in the interest of

- Warding off cyber attacks
- Facilitating safe travel
- Collecting taxes where due
- Countering the financing of criminals
- Promoting a safe environment

Proposed Solution:

Element 4 –
Allows audits of how data is treated

Auditing of governments' activities
Government may need access to data…

Nonetheless, still want accountability. Since requires secrecy, need internal checks and balances. Can these be designed into the system?

Proposed Solution:

Element 4 –
Allows audits of how data is treated

Auditing of governments' activities
MIT's Transparency and Policy Aware Web

- Deals with government treatment of data.
- For more info, see http://publications.csail.mit.edu/abstracts/abstracts06/djweitzner2/djweitzner2.html

Proposed Solution:

Element 5 –
Affords a mechanism for redress

Qualities

- Based on common global understanding
- Accessible
- Efficient
- Effective

OECD Role?

Mechanism for redress

Model in WIPO's Arbitration and Mediation Center?

Could the OECD or another international body offer such services in the data protection context?

Thank you.