IGF 2006 – Athens
Privacy Workshop I

International Data Protection and Digital Identity Management Tools

Mary Rundle
mrundle[at]cyber.law.harvard.edu
InfoCard Limitation:

Does not say what happens to data once transferred.
Challenge:

How to bridge international, personal data protections and digital identity management tools
Express user preferences in a way that:

1. Observes international data protection standards;
2. Is clear and easy for people;
3. Hooks into the identity management infrastructure; and
4. Allows audits of how data is treated.
1. **International data protection standards**


   - Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Council of Europe, 1981)

   *Echoed in Montreux Declaration (Data Protection and Privacy Commissioners, 2005)*
Principles:

1. Collection Limitation
2. Data Quality
3. Purpose Specification
4. Use Limitation
5. Security Safeguards
6. Openness
7. Individual Participation
8. Accountability
2. **Is clear and easy for people**

Creative Commons-like icons:
- Human readable
- Lawyer readable
- Machine readable (globally)
<table>
<thead>
<tr>
<th></th>
<th>You agree not to use this data for marketing purposes.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>You agree not to trade or sell this data.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>You allow me to address inaccuracies in the data and request its removal.</td>
</tr>
<tr>
<td></td>
<td>You agree to take reasonable steps to keep my data secure.</td>
</tr>
<tr>
<td></td>
<td>You agree to arrange with X organization to help resolve any disputes we have over your treatment of this data. [The seal / name of the entity follows.]</td>
</tr>
</tbody>
</table>
Advantages:

- Bridges jurisdictional requirements.
- Offers simple choices.
- Allows multiple combinations according to context.
- Works internationally.
3. Hooks into the identity management infrastructure

Higgins’ (open source, Eclipse):

- Allows interoperability in i-card tools
- Overlays different systems
For more information on Higgins, see:

http://www.boston.com/business/technology/articles/2006/02/27/harvard_tech_firms_push_data_privacy/
4. Allows audits

• Checks against abuse by private actors having access to data.

• Checks against abuse by governmental actors having access to data.
Government may need access to data, e.g., in the interest of:

- Warding off cyber attacks
- Facilitating safe travel
- Collecting taxes where due, and
- Countering the financing of criminals

Nonetheless, still want accountability. Since requires secrecy, need internal checks and balances.
Bandit's audit capabilities:

- Meant to allow audit of private actions.
- Fully open source and developed in public.
- Component is the Audit Record Framework (ARF).
For more info on Bandit, see:

- [http://www.bandit-project.org/index.php/Compliance_Records](http://www.bandit-project.org/index.php/Compliance_Records)
- [http://www.bandit-project.org/index.php/Architecture_and_Design](http://www.bandit-project.org/index.php/Architecture_and_Design)
MIT’s Transparency and Policy Aware Web

So far deals with government treatment of data.
For more information on MIT’s PAW project, see:

http://publications.csail.mit.edu/abstracts/abstracts06/djweitzner2/djweitzner2.html
(Review) Express user preferences in a way that:

1. Observes international data protection standards;
2. Is clear and easy for people;
3. Hooks into the identity management infrastructure; and
4. Allows audits of how data is treated.
Other Information:

• Draft paper on topic in general:

• Paper on interaction of some international legal provisions and InfoCards:
  http://cyber.law.harvard.edu/home/2006-01
Thank you.