Position Paper Submitted for the W3C Workshop on
Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement
17 and 18 October 2006 -- Ispra/Italy

International Personal Data Protections and Digital Identity Management Tools

Mary Rundle[1] – 13 September 2006

Microsoft, Sxip, the Liberty Alliance, Shibboleth, Passel, Higgins, and other technology companies and designer groups have been actively working to build a new digital identity management system (or system of systems) to provide greater certainty and efficiency in online dealings. While many are touting the benefits of user-centric digital identity management, to date discussion has largely ignored the questions of what data, exactly, should be under the user's control, and how the user's preferences for the treatment of that data can be expressed and subsequently enforced.

The goal is to equip the individual with control over his personal data, in a way that allows information exchanges to flourish for a healthy society. To help advance this goal, this position paper focuses on one particular area at the intersection of law and technology – that is, international personal data protections and digital identity management. The paper briefly breaks this challenge into discreet chunks that experts from a range of disciplines might take up as they work in loose collaboration. These discreet chunks or pieces of the puzzle include:

1. Determining what data should be under the user's control
2. Expressing user preferences for the treatment of personal data
    a. In a manner that observes international legal guidelines
    b. By using Creative Commons-like icons
    c. That hook into the identity management infrastructure
3. With the actual treatment of data then being auditable by electronic means

1. Determining what data should be under the user's control

The question of what personal data, exactly, should be under the user's control is not a new one, though an internationally acceptable stance on this subject has yet to obtain consensus. In fact, the lack of agreement on this score has given companies a certain sense of immunity from the charge that they should do something to guarantee personal data protection: for if there is no commonly accepted notion of what rights a person has, it would be unreasonable to expect companies to design technologies to accommodate these amorphous rights.

The question of what constitutes personal data and confers a user right of control is arguably a political one that will take time to resolve. While obviously important, this issue nonetheless need not impede work on other pieces to the puzzle. An expedient way to handle this issue in the meantime may be for users, service providers, and other parties involved in transactions to set out contractual terms that specify how personal data will be treated.

2. Expressing user preferences for the treatment of personal data

a. Observing international legal guidelines

[1] Mary Rundle is a Fellow at the Berkman Center for Internet and Society at Harvard Law School and a Non-Resident Fellow at the Center for Internet and Society at Stanford Law School. This paper was produced under the Net Dialogue project.

In approaching this overall puzzle, it will be important to bear in mind that personal data will be flowing across, processed in, and stored among different jurisdictions. To keep costs down, parties will want to know that they meet the requirements of the various jurisdictions.

A number of international arrangements speak to the protection of personal data. Notable legal principles include those found in the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (adopted by the Organization for Economic Cooperation and Development, or OECD, in 1980), and the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (adopted by the Council of Europe in 1981). These instruments comprise a solid list of protections regarding personal data collection, storage, and processing. Principles include collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.

While jurisdictions may vary as to what default rules apply, icons may solve this conflict by allowing users to choose directly how their data should be treated. In order to ensure that a mechanism for users to express preferences is user-friendly, options will need to be clear, easy to choose among, and understandable in different combinations (since different combinations may be chosen for different contexts). In this regard, complex, international legal requirements will need to be boiled down to a few, simple choices that can be combined in different ways to suit different purposes, according to context – with these choices then represented as icons.

So, for example, a person might choose a different suite of icons for the transfer, use, and storage of his health records than for his favorite music playlists. Even simplified into six choices, the possible combinations may be too confusing to many user's tastes. For this situation, it may be that people will elect to rely on the recommendations of others. To use the same example: a person might opt for the national medical association's recommended set of icons for health records, but for an indie music club's suggested suite for his playlists.

A team of international lawyers specialized in personal data protection have been exploring how to distill legal principles into simple form while still retaining their meaning and accomplishing their intended impact.

Of course, in addition to international legal standards for the protection of personal data, there are also government policies that seem to cut in the other direction from user control over personal data. These policies are often geared more toward areas of legitimate government interest in accessing and sharing users' personal data – for example, warding off cyber attacks, facilitating safe travel, collecting taxes where due, and countering the financing of terrorists or other criminals. In other words, there are two very different scenarios leading to different requirements for the treatment of personal data: one in which an individual has a right to see that his preferences are honored, and another in which a government has authority to commandeer people's personal data. While these situations may seem at odds with each other, electronic audit tools, referenced in Section 3, below, may be able to reconcile them.

b. Using Creative Commons-like icons

Creative Commons has developed a method of visually representing a user's select set of choices, in its case with respect to elements of copyright.[2] In the case of personal data, what we are seeking is something similar, where a user can decide among a range of options that express his particular preferences regarding the treatment of his personal data.

As presented by Creative Commons, these choices that are symbolized by icons are elaborated in a prescription that is "human readable," "machine readable," and "lawyer readable."[3] Applied to our context, a user's set of choices regarding the treatment of his data would be expressed in lay terms that he could understand, in metadata that machines could respond to, and in legal terms that the judicial system could recognize.

c. Hooking into the identity management infrastructure

Several designers and others interested in user-centric identity management have taken steps to form a new Identity Commons association.[4] One working group that is convening will deal with so-called "identity rights agreements." Drawing on the association's expertise in the technical architecture of new identity management systems, this group will aim to develop "a small initial set of identity rights agreements, each referenceable using a persistent identifier."[5]

Naturally, the association welcomes participation from a wide range of stakeholders with specialized interest in identity management.[6]

3. With the actual treatment of data being auditable by electronic means

The ability of a user to express his preferences is of little value if these preferences cannot be enforced. Similarly, government interest in having access to people's personal data will not be able to serve the common good if such power can be abused. An enforcement mechanism is therefore needed to safeguard the treatment of personal data by private as well as public actors.

An approach that might serve here is one called "Transparency and the Policy-Aware Web", or PAW, which is being pursued by the Computer Science and Artificial Intelligence Laboratory at the Massachusetts Institute of Technology.[7] Simply stated, this technology provides a sort of audit capability to ensure that the government acts properly in handling personal data. While PAW is being conceived as a litigation tool in judicial proceedings where prior governmental conduct is at issue, the technology would seem to have other applications as well. For example, it would seem this technique could be applied beyond the court setting to verify that actors complied with personal data protection standards, be those actors governmental or private.

---

[2] See http://creativecommons.org/about/licenses/comics1 (viewed on 13 September 2006).
[3] See http://creativecommons.org/about/licenses/how2 (viewed on 13 September 2006).
[4] See description of association at http://wiki.idcommons.net/moin.cgi/FrontPage (viewed on 13 September 2006.
[5] See draft working group charter at http://wiki.idcommons.net/moin.cgi/IdentityRightsAgreementsCharter (viewed on 13 September 2006).
[6] Please contact Dan Perry (dan [at] danielperry.com).
[7] See http://publications.csail.mit.edu/abstracts/abstracts06/djweitzner1/djweitzner1.html (viewed on 13 September 2006).

Conclusion

Together, might these pieces of the puzzle allow an individual to have greater say over what happens to his personal data – giving him effective notice, choice, access, and security – while at the same time permitting accountable government overrides where necessary? Might these tools enable a sort of "legal interoperability" that accommodates different jurisdictional requirements for the protection of personal data, while at the same time facilitating efficient web exchanges according to user desires?

Again, the goal is to equip the individual with control over his personal data in a way that allows information exchanges to flourish for a healthy society. By collaborating in a multi-disciplinary team, technologists, international policymakers, and other enthusiasts may find ways forward.

If you would like to participate in this exploration, please contact Mary Rundle (mrundle [at] cyber.law.harvard.edu).