CENTER FOR INTERNET AND SOCIETY
AT STANFORD LAW SCHOOL

Research Publication No. 2006
June 2006-06

International Personal Data Protection and Digital Identity Management Tools

Background Paper for Identity Mashup Conference – June 19-21, 2006
Hosted by the Berkman Center for Internet and Society at Harvard Law School
20 June 2006, 11am-12:30pm – Track A Panel Session

Mary Rundle

JEL Classification: K330, O330, O380

INTERNATIONAL PERSONAL DATA PROTECTION AND DIGITAL IDENTITY MANAGEMENT TOOLS

Mary Rundle*

ABSTRACT

International guidelines establish principles for the treatment of personal data. Might digital identity management tools simultaneously allow the interests of government, the private sector, and the citizen to be met - namely, legitimate government access to and sharing of personal data, efficiency in web-services exchanges, and effective protections for personal data?

Keywords: Personal data protection, identity management, policy-aware web.

* This paper has been produced under Net Dialogue, a project funded by the Lynde and Harry Bradley Foundation and jointly sponsored by Harvard's Berkman Center for Internet and Society (Berkman Center) and Stanford's Center for Internet and Society (CIS). Net Dialogue seeks to shed light on international governance of the networked world and to promote dialogue between the technology and international policymaking communities, with a view to promoting democracy in the Information Society. Mary Rundle is a Fellow at the Berkman Center and a Non-Resident Fellow at CIS.

INTERNATIONAL PERSONAL DATA PROTECTION AND DIGITAL IDENTITY MANAGEMENT TOOLS

By Mary Rundle

Some international legal instruments call for the protection of personal data as it flows internationally; meanwhile, others establish a legal basis for the access and sharing of such information by governments (often with the help of private sector entities). Complicating the situation further are differences in jurisdictions' approaches to these issues.

On the technological front, new digital identity management tools may affect the ability of entities to meet different legal requirements in their treatment of personal data. At the same time, electronic auditing techniques may allow parties to verify compliance.

Might these tools simultaneously allow the interests of government, the private sector, and the citizen to be met – namely, legitimate government access to and sharing of personal data, efficiency in web-services exchanges, and effective protections for personal data?

Various international arrangements call for the protection of personal data. Examples that stand out include 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 initiatives 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.

More recently, governments have been involved in other negotiations that would seem to cut in the other direction. That is, rather than calling for the protection of personal data, their focus is more on other challenges that give rise to a legitimate government interest in accessing and sharing personal data. For example, in fighting cybercrime, governments want authority to require Internet service providers to hand over subscriber information, among other data. To facilitate travel, governments have agreed to certain standards for a global system of electronic identity confirmation. For taxation of international e-commerce, OECD members are seeking reliable ways to identify taxpayers. To counter the financing of terrorists or other criminals, governments seek to ensure that information on originators of wire transfers is available.

Meanwhile, Microsoft, Sxip, the Liberty Alliance, Shibboleth, Passel, and other technology companies and consortia have been actively working to build a system of digital identity management tools to provide greater certainty and efficiency in online dealings.

On a related front, the MIT's Decentralized Information Group[*] has been working on what it calls "Transparency and the Policy-Aware Web", or PAW. 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 is conceivable that PAW could be used to look into activities by private entities. In addition, it would seem this technique could be applied beyond the court context for verifying that actors comply with personal data protection standards.

In combination, will these legal provisions and tools allow an individual to have greater say over what happens to his personal data – giving him effective notice, choice, access, and security? Will the combination of law and technology enable government to access and share personal data in the name of legitimate purposes, while at the same time preventing the misuse of data? Will these tools enable a sort of "legal interoperability" that accommodates different legal requirements regarding the protection of personal data and government uses of it, while enabling efficient web services?

[*] At the Computer Science and Artificial Intelligence Laboratory of the Massachusetts Institute of Technology.