INFORMATION
INTEGRITY
SOLUTIONS

BRIEFING PAPER

USER CENTRIC, LAYERED, AND GLOBAL:
WHAT SORT OF POLICY AND LEGAL FRAMEWORK?

BY MALCOLM CROMPTON

For: Oxford Internet Institute: Workshop on

A POLICY AND LEGAL FRAMEWORK FOR IDENTITY MANAGEMENT

2 APRIL 2009

1 INTRODUCTION

There are a number of privacy and trust challenges for managing identity on the internet. The policy and legal issues are complex and frameworks to handle them are only slowly evolving. Governments and other organisations are finding that addressing domestic issues only solves half the problem. This is because managing e-identity is rapidly becoming a global as well as a domestic issue. Whether domestic or global there is clear evidence that one of the keys to unravelling a number of the conundrums is the need for a stronger focus on the user in developing frameworks.

2 THE GREAT RISK SHIFT

Users are starting to realise that when an organisation moves its service to the online environment, the organisation often manage their own risks by shifting the risks on to the individual. In the context of identity management solutions, this "great risk shift" often means:

- Stringent requirements are placed on individuals to identify themselves, but no attention is paid to assuring the individual that the organisation is who it says it is (ie no provision for mutual trust);
- Little attention is paid to the security and secondary use risks from the greater ease of aggregating data about an individual through the use of unique identifiers;
- Little attention is also paid to the consequences of the huge volume of peripheral data that could be collected through the digital footprint every time individuals electronically identify themselves;
- The inconvenience for individuals (or worse) if the system fails or when individuals loses their means of identifying themselves.

3 CURRENT APPROACHES FALL SHORT

A number of attempts to adopt identity management solutions have also run into trouble with the community because they have not been sensitive to the impact that identity management initiatives may have on the ability of users to exercise control over their lives and their identities. This is often blamed on an undue focus on the technology of the proffered solution and only from the point of view of addressing the needs of the organisation. Regulation of e-identity has tended to focus on compliance with existing (and rapidly becoming outdated) law, or only on changing existing laws so that current impediments can be circumvented.

Part of the answer does lie in technology and in the law but there are also some other, more nuanced strategies that must come into play to create the trust in new identity management solutions.

4 USER CENTRIC IDENTITY MANAGEMENT ONE KEY

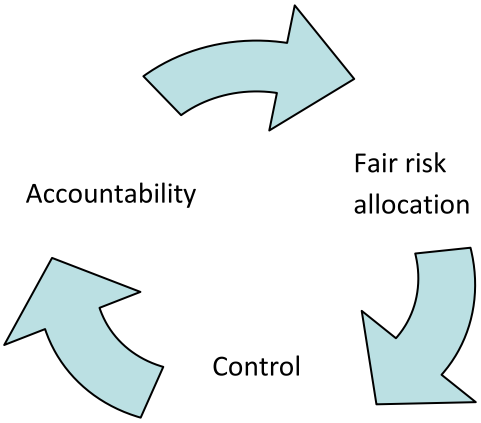
There is an increasing body of thinking around what has become known as the 'user centric' approach to identity management. Early work includes reports from the London School of Economics (LSE) in response to the UK Identity Card proposals, Microsoft's Kim Cameron's 'Laws of

Identity' and the work Information Integrity Solutions.[1] More recently, we have seen commercial investment in such solutions, including the purchase by Microsoft of the U-Prove technology[2] and the inclusion of the Idemix technology in the Higgins Open Source Identity Framework[3]. The European Commission and its research partners in the academic & commercial sectors are also investing significantly in user centric ID management including in the PRIME & PrimeLife projects[4].

Our analysis suggests that organisations must consider three dynamic factors from the point of view of the individual to encourage mutual trust. These are:

- **Fair risk allocation** – ensuring that individuals understand the risks and are confident that they are fairly allocated to the party most able to bear them;
- **Control** – ensuring that individuals have the control they want over how information is demanded, collected and stored, or if that is not possible or wanted, they understand the organisation and are confident that it will handle the information appropriately;
- **Accountability** – ensuring that the organisation is accountable and transparent about how it will handle personal information and take appropriate responsibility for dealing with the impact of failure on the individual including having a good safety net.

These factors are dynamic and interdependent. All components must be addressed from the user's point of view to achieve trust, but some may need more emphasis depending on the circumstances. For example, where people perceive a high level of personal risk, they may demand increased personal control. On the other hand, where an organisation displays high levels of accountability, including transparency, individuals may perceive that there is less risk, and may demand less levels of direct personal control.



[1] "The Identity Project, An assessment of the UK Identity Cards Bill and its implications", Chapter 18, 'Design Principles and Options', London School of Economics, June 2005 (http://is2.lse.ac.uk/idcard/; "The Laws of Identity", Kim Cameron, May 2005 (http://msdn2.microsoft.com/en-us/library/ms996456.aspx); "Proof of ID required? Getting Identity Management Right", Privacy Commissioner Malcolm Crompton, March 2004 (www.privacy.gov.au/news/speeches/sp1_04p.html); "Trustguide", a Sciencewise programme funded by the Office of Science and Technology in the UK Department of Trade and Industry, October 2006 (www.trustguide.org.uk).

[2] See www.microsoft-watch.com/content/security/microsoft_says_u-prove_it.html and www.identityblog.com/?p=934

[3] See http://wiki.eclipse.org/Idemix_Provider.

[4] See www.PRIME-project.eu and www.PrimeLife.eu respectively

How these dynamics play out may depend on the legal, historical, cultural environment, including whether the organisation is public or private sector and the purpose for which identity management is being implemented.[5]

5 LAYERED DEFENCE STRATEGIES NEEDED

Instead of relying only on technology, or on a very narrow, one size fits all use of law, it would seem more advisable to apply a 'layered defence' approach that draws upon a combination of the following tools as necessary and appropriate to achieve both the goals of the project and the privacy needs of individuals and society as a whole.

- Education of individuals, both citizen users and staff, about risks and how to manage them ;
- Ensuring there are appropriate laws in place particularly where privacy risks are very high (for example, specifically limiting use and disclosures, providing criminal penalties for misuse if necessary) and providing special measures to manage change;
- Technology (for example, limiting information collected and who has access to it);
- Governance, including transparency and accountability (this can be a combination of policy, procedure technology and law and will often rely on technology to produce audit information);
- Safety mechanisms for citizen users when systems or services fail.

Such a layered defence approach is applicable at the local, national and global context. It goes without saying that implementing these mechanisms in a global context adds another layer of complexity. To start with governments are only just coming to terms with the implications of managing identity in a global context. The work of the OECD and APEC to put in place a global governance framework for the transborder flow of personal information is just the tip of the iceberg. Commercially developed federations of identity are contributing, but a major question remains as to whether this is sufficient.

[5] For further development of this analysis see a white paper called 'Safe to Play' which Information Integrity Solutions wrote with Cisco, available at www.iispartners.com/Publications/index.html#Yr2007.