

# Beyond Security: Implications for the Future of Federated Digital Identity Management Systems

**Christine Satchell**

University of Melbourne  
Parkville, 3010 Australia  
satsc@unimelb.edu.au

**Graeme Shanks**

Monash University  
Clayton, 3080, Australia  
Graeme.shanks@infotech.monash.edu.au

**Steve Howard**

The University of Melbourne  
Parkville, 3010 Australia and  
Department of Computer Science  
Aalborg University, Aalborg  
showard@unimelb.edu.au

**John Murphy**

Novell Pty Ltd, Australia  
John.Murphy@novell.com

## ABSTRACT

Federated identity management is often viewed by corporations as a solution to support secure online commerce by synthesising complex and fragmented user information into a single entity. However previous research (Satchell et al 2006) has revealed a new set of end user needs for the design of identity management systems. This paper explores these needs from an identity management provider perspective, finds both alignment and divergence in needs and identifies a generational shift as a major cause of the differing needs. Whilst X and Y generations do not react strongly to concerns about digital identity theft or misappropriation of information, they seek to create and control their digital representations to be streamlined, portable across domains and revealing elements of their real life identity. There is still a considerable challenge for providers who must look beyond 'security' and 'authentication' to include 'user control', 'synthesis', 'portability' and 'personalisation' in the design of their systems.

## Author Keywords

Digital identity, federation, security.

## ACM Classification Keywords

H5.2. User interfaces

## BACKGROUND

The convergence of technologies and services has resulted in users conducting a growing range of activities, transactions and interactions in a variety of digital environments. In order to provide seamless access across technologies and services, federated systems have been introduced. Supported by multiple organizations, they allow identity and the ensuing entitlements to be portable across domains (Clarke 2004).

Liberty Alliance (2003) lists the benefits of federated identity as a more satisfactory online experience for the end user including new levels of personalisation, security

and control; the enabling of service providers to easily and securely provision accounts and provide access privileges; and the opportunity for businesses to create new relationships with each other and realise business goals at lower cost. However Clarke (2004) argues that only a limited degree of personalisation, security and control are extended to the end user. Furthermore, he notes the other cited benefits are largely from the business perspective and asks why should the customer provide their identity information?

Service providers argue that from the user's perspective, federated systems offer a streamlined, consolidated representation of the person's digital data, allowing the user to gather multiple identities together under one umbrella. For example, rather than requiring the user to remember numerous login details, only one user name and password is required (Gengler, 2004). It can be seen that in a fragmented digital world, this goal of developing standard online identities not only provides users with vital cohesion, but contributes to digital environments that are easily traversable spaces. Less explored in the literature is whether or not these changes are generating a new set of user needs. Furthermore, the body of research that critically examines organisations' attempts to federate peoples' digital identities provides few insights into what users themselves really want, or how the user needs could align with those of the identity management providers. This research is part of a project that has identified and explored some of these issues.

## RESEARCH DESIGN

This research is the third and final part of a study of user needs in relation to identity management. The first part of the study entailed a study of literature aimed at uncovering concerns and needs of customer or citizens - the "demand" side of identity management. The following six key issues emerged.

- Control and power over identity including the ability to create, maintain and share information related to identity.
- Authentication and the ability to remain anonymous during transactions

OZCHI 2006, November 20-24, 2006, Sydney, Australia.

Copyright the author(s) and CHISIG

Additional copies are available at the ACM Digital Library (<http://portal.acm.org/dl.cfm>) or ordered from the CHISIG secretary (secretary@chisig.org)

OZCHI 2006 Proceedings ISBN: 1-59593-545-2

- Trust in relation to furthering commercial relationships and the link between the ability to control a digital identity and the development of trust between parties
- Security and the problems with aligning legislation and commercial responsibility with the fast pace of developing identity technology
- Privacy and the balance between governance, legal needs and national security on the one hand, and individual dignity and privacy on the other; and
- Multiple Identities that may overlap, yet need to be maintained and segregated in different contexts

The second phase was an empirical study of end users involving 15 open-ended interviews, two focus groups with seven participants each and a cultural probes study of five users. The two main themes to emerge were the need for multiple digital data sets that are moored to a central identifier, and the need for control over these data sets (Satchell, et al. 2006).

The third phase explores the reactions of identity management provider personnel to the user needs discovered in the first two phases. It comprised of a focus group with five participants, drawn from industry. They were all from organisations significantly involved in identity management with some participants representing the 'customer facing' part of the business and others representing the 'system design' part of the business. The focus group data was analysed to identify alignment and differences with the user needs.

### **CONVERGENCE BETWEEN END USER NEEDS AND THE PROVIDERS' PERSPECTIVE**

This section explains how two user needs that emerged from the end user study converge with the needs of providers.

#### **End user need: multiple identities that are also streamlined and portable**

Digital identity it is not singular or static, rather it is characterized by its multiplicitious nature. Users can take on many different personas in accordance with the nature of the activity they are conducting or the person with whom they are interacting (Claube & Kohntopp 2001). However, this did not necessarily translate to the need for disparate or separate silos of data. Rather, there was a need for the fragments to be moored to the user's central self. Even when participants' professed an ideological opposition to organizations compiling data about them, in practice, they were actually quite blasé about keeping information in one place for the sake of convenience.

Multiple digital identities should not be thought of as disembodied entities, but as part of the cohesive whole that forms the meta-identity of the person. This is especially relevant because digital environments themselves are rapidly evolving into integrated systems that include mobile phones, the Internet, digital television, gaming, mobile phones and e-commerce. Users are provided with highly personalised and tailored services, yet most identity management systems still support digital identities that are silos of information, context specific and cannot be moved around. For

example, one of the most valued identities on the net is an eBay reputation, yet it exists purely on eBay and cannot be moved or 'mashed' onto Craig's list (Hardt, 2005)

#### **Providers' perspective**

Federated identity management systems offer more than silos of information. They offer the potential for much needed synthesis of previously fragmented data sets (Clarke, 2001). Yet the customer facing providers in the study reported that a major concern with digital identity management was that even within one company, users will have different identities and they are not easily consolidated. For example P4 noted that within the Telco where she worked a user might have an Internet, mobile phone and land line account. Each of these represents a different identity and while P4 wished she could extend federation to the user by for example, offering streamlined billing, the infrastructure would not allow it.

People have different identities, they give you different details but they are the same person. From a customer experience perspective you might have several applications on a member and none of those talk with each other. They are all separate identities and that is a huge problem. (P4)

In commercial industry there are many separate legacy systems that have significant and sometimes insurmountable integration issues. In this way users maintain multiple identities however they are neither streamlined nor portable. When exploring this user need from the system designer perspective there were reservations about infrastructures that would facilitate this sort of streamlining. There was a propensity to avoid the centralisation of information for security reasons.

In relation to identity, as soon as you make something more useful by making it more universal you narrow the focus of attack. (P6)

A consolidated single source of identity information that may be applied across services and domains provides a single focus for an attacker attempting to steal an identity. In this way a consolidated identity is streamlined and portable, yet more vulnerable from a security perspective.

#### **End user need: control over personal information**

Despite the potential benefits of federation, in the user needs study users were less likely to disclose information if they lost control over it. Different types of control relating to three broad and overlapping phases – 'hatch', 'match' and 'dispatch' – were identified.

##### *Hatch*

The 'hatch' phase relates to the way digital identities are born, or evolve. Participants expressed strong views on the active role they desired in that creation process and the strong relationship that their digital identities should have with their 'real' or non-digital identities.

##### *Match*

The 'match' phase relates to the way digital identities, especially when federated, are networked collations of identifying and related information. The emergent properties of these information networks may include more thorough and complete pictures of end users than many are comfortable with. Conversely, the desire to

restrict information was contrasted by the need to reveal highly personalized information with users indicating digital disclosure can become more meaningful when elements of everyday life are incorporated.

#### *Dispatch*

The 'dispatch' phase relates to the way in time digital identities become obsolete, or their continuance is undesirable for some reason. Participants expressed feelings of powerlessness in their ability to 'kill off' a digital self. This is vital because it completes the digital identity lifecycle.

#### **Providers' Perspective**

In relation to the 'hatch' phase, the user need to actively create one's own digital identity aligned with the customer facing providers, who noted that information collected about the individual from the individual better positioned the organization to meet the customer's needs. Furthermore, in keeping with Hagel and Rayport (2000) they noted that the information about the user, provided by the user, was itself, a valuable acquisition.

The user need to restrict or compartmentalise information in the 'match' phase, reflected the vision of the providers from the system design perspective who were concerned with creating federated digital identities systems that limit information. They were focused on reducing what is revealed to minimize risk and ensure that incorrect information was not accessed. P6 stated, "It does not follow that information is attached to identity." This means that while mini-pieces of information may reveal small and limited facts about our identity, they are not enough to be used to determine the complete picture of the user's identity. While P3 noted that a feature of federated systems was their ability to maintain "multiple discrete identities". On the other hand, the user need to reveal more information about one's self aligned with the needs of the providers from the customer facing point of view who were concerned with digital identity in terms of capturing as much information as possible. "You are not just after the identity of the person. You are also after who they are and who they actually care about." (P5)

In relation to the 'dispatch' phase, all participants in the providers study agreed that the ability to terminate a digital identity was important.

As people gather more and more information from you they can construct a virtual you or representation of you. Given that we have multiple identities, how sticky are they, how difficult is it for people over period of time to create a complete new set of identities, and how persistent are they over time? (P7)

This means that while all participants agreed it is important to terminate an identity, it is unclear how long identities persist, and how they may be terminated or replaced.

#### **DIVERGENCE BETWEEN END USER NEEDS AND THE PROVIDERS' PERSPECTIVE**

This section explains how user needs diverge from the needs of two groups of providers: the customer facing group and the system designer group.

#### **End user and customer facing provider perspectives**

Both customer facing providers and users aimed to achieve a customer experience that was personalised to meet the needs of the individual. The overriding goal was convenience.

Customers want an overwhelming sense of convenience. They want easy use. They have a lot of things on and have many identities across different sectors in life. They want these identities to be streamlined and convenient. (P5)

This does not mean that security was not an issue. Indeed it is the trust that both users and providers in a customer facing role had in digital identity management systems that allowed practical concerns - such as identity theft and ideological concerns that an organisation might have big brother type control over personal information - to be overcome.

Certainly when someone needs to access any of our applications we have someone at an external organization that authenticates or validates who they are (P5)

Reputable organisations see the protection of personal information as crucial to an organisation's reputation. P4 stated "Privacy is a huge thing for us: we will never share information." This was supported by P5 "Never, ever share information with anybody else - won't go there." This aligns directly with the strong end user expectations that privacy and ethical management are paramount.

#### **Provider perspective: system designer**

Although a focus on security was important for users and all providers, the system designers have a strong understanding of the repercussions and thoroughly investigate worst case scenarios.

If someone gathers bits and pieces of information they start having a basis ... If they have alternative motives, the more that they know about you, the more they can represent themselves initially at lower levels. They might get an electricity bill in your name, car registration or something like that, and then build it up into something more substantial.

In summary, for system designers identity management is primarily about authentication and minimising risk. In contrast, customer facing providers, aligning more with end users, understand the importance of convenience and streamlining. Customer facing providers also understand the importance of security in terms of maintaining the reputation of their organisation and thus, the trust of end users.

#### **GENERATIONAL SHIFT**

During the providers' focus group a new theme emerged that was based on the disjunction between the need for security and the need for more dynamic digital identities. A 'younger generation' was referenced with different attitudes towards security and privacy. Further analysis of the data in the first two parts of this research indicate that this could largely be attributed to generational shift as Gen X and Y move away from the 'big brother' Orwellian notions of privacy that characterized the baby boomer generation. This was subsequently agreed upon by all the participants in the provider study.

The older generation are more concerned about having multiple identities. But maintaining separate identities or personalities everywhere takes time. The younger generation is not that concerned about having multiple silos. (P6)

Furthermore, as the risks become well established and are understood, a new generation of users tend not to react strongly to concerns about digital identity theft or misappropriation.

I've spoken to a lot of kids who have no problem in sharing identity and details about themselves. I know no one's parents or grandparents that will do any of that. (P3)

The research revealed that increasingly savvy users know that financial losses due to crime such as stolen credit card details are generally shouldered by institutions such as banks. This is in direct contrast to the older generation who believe they would shoulder the complete burden of financial loss due to identity theft. Also, the impact of loss of reputation due to the unauthorised access and dissemination of personal information has become diluted in a society saturated by reality television, personal blogs and Flickr. Gen X and Y will use these multiple channels at their disposal to fight loss of reputation. This is in direct contrast to the older generation who do not feel that they had control over channels through which reputation was presented and disseminated.

Rather than *conceal*, Gen X and Y want to *reveal* elements of their real life identity, which is increasingly merging with their digital life. In order to respond to this, these users seek out *streamlined* systems allowing *portability* across domains to forge identities as seamless as physical world tasks. Yet, it is the limitations of the digital identity systems themselves that are inhibiting this from happening. Networked societies present immense opportunities for the flow of commerce, however, the 'siege mentality' which characterise efforts to secure perimeters actually creates barriers which prevent users from increasing their activity (Windley 2005).

#### **CONCLUSION: BEYOND SECURITY**

The increasing integration of digital environments in the personal spheres of the general public has led to a corresponding evolution in societal concerns. While preoccupations at the time of the early digital society in the 1970's and 1980s's centered around concerns of privacy, anonymity, and resistance to the threat of a culture of surveillance, our research finds that end users today assume security and trust reputable organizations to treat personal information in an ethical way.

In the early 21<sup>st</sup> Century, at a time when technologies allow the worst case scenarios described in Huxley's *Brave New World* and Bradbury's *Fahrenheit 451*, users are less concerned about issues of digital identity theft or misappropriation of information. This does not erode the need for service providers' to tend to these dangers. To the contrary, deploying robust personal digital identity management systems is the cornerstone of security. It is the next set of needs that form the building blocks that must now be addressed.

Providers, designers and architects of identity management systems must keep up with the demands of the public and address the needs and desires being voiced by a new generation of user. Rather than hide and restrict information about them, the digital generation instead seeks to create, manipulate, control, and even play with, digital representations of themselves as projected to commercial entities, or to their immediate personal circles. This was noted by Boyd in her seminal paper on digital identity management (2004).

In computer-mediated communication (CMC), the performance of identity occurs primarily not through direct experience of the body but within the constraints of digital representations constructed by interactive systems. To compensate for the loss of physical presence, people have had to create new ways of reading the signals presented by others, and new ways to present themselves.

This paper has presented a challenge that will be faced by designers of future digital identity management systems. Now that satisfying the need for 'security' is taken for granted, digital identity management must start to support fluid user driven models that begin to include 'user control', 'synthesis', 'portability' and 'personalisation'.

#### **ACKNOWLEDGEMENTS**

Thanks to participants in the empirical study and to Elizabeth Hartnell-Young for her assistance with the data collection. The research is funded by the Australian Research Council and Novell through Linkage Project LP0347459 'Humanising the Convergence of ICTs'.

#### **REFERENCES**

- Boyd, D. Representations of Digital Identity Representations of Digital Identity. CSCW 2004 workshop: November 6, (2004), Chicago
- Carroll, J. M. *Human Computer Interaction in the New Millennium*. NY and Boston: ACM Press & Addison Wesley, (2002).
- Clarke, R. Authentication: A Sufficiently Rich Model to Enable e-Business, Xamax Consultancy, (2001), Accessed 6th June, 2004  
<http://www.anu.edu.au/people/Roger.Clarke/EC/AuthModel.html>
- Gengler, B. Standard ID clears a path in password jungle, IT Alive Section, The Australian, August 3rd (2004), 4
- Heardt, D. Web 2.0 High Order Bit - Identity 2.0, (2005), [http://identity20.com/media/WEB2\\_2005](http://identity20.com/media/WEB2_2005)
- Hagel, J. and Rayport, J. The Coming Battle for Customer Information, Harvard Business Review, January-February, (2000), 53-65
- Liberty Alliance Project. Introduction to the Liberty Alliance Identity Architecture, Revision 1.0, March, (2003) (accessed 5 August 2004)  
<https://www.projectliberty.org/resources/whitepapers/LAP%20Identity%20Architecture%20Whitepaper%20Final.pdf>
- Satchell, C., Shanks, G., Howard, H., Murphy, J. Knowing Me Knowing You – User Perceptions of Federated Digital Identity Management Systems. Proc. ECIS, Gothenberg, Sweden, June (2006).
- Windley, P. *Digital Identity*. O'Reilly & Associate (2005)