

This is the author-manuscript version of this work - accessed from <http://eprints.qut.edu.au>

SATCHELL, CHRISTINE AND SHANKS, GRAEME AND HOWARD, STEVE AND MURPHY, JOHN (2006) 'KNOWING ME – KNOWING YOU. END USER PERCEPTIONS OF DIGITAL IDENTITY MANAGEMENT' SYSTEMS. IN *PROCEEDINGS ECIS, GÖTEBORG, SWEDEN.*

Copyright 2006 (please consult author)

## KNOWING ME, KNOWING YOU: END USER PERCEPTIONS OF IDENTITY MANAGEMENT SYSTEMS

Satchell, Christine, The University of Melbourne, Parkville, 3010 Australia, [satc@unimelb.edu.au](mailto:satc@unimelb.edu.au)

Shanks, Graeme, Monash University, Clayton, 3080, Australia,  
[Graeme.shanks@infotech.monash.edu.au](mailto:Graeme.shanks@infotech.monash.edu.au)

Howard, Steve, The University of Melbourne, Parkville, 3010 Australia, [showard@unimelb.edu.au](mailto:showard@unimelb.edu.au)  
and Department of Computer Science, Aalborg University, Aalborg

Murphy, John, Novell Pty Ltd, Australia, [John.Murphy@novell.com](mailto:John.Murphy@novell.com)

### Abstract

*Federated identity management systems synthesise complex and fragmented user information into a single entity. Literature from the identity management system providers note this integration extends many benefits to the end user and the privileges provided by digital identity authentication schemes have been well documented from this perspective. Less explored however, are the perceptions of federation from the user's perspective. This paper attempts to address this gap by reporting on an empirical user study that examines the relationship between identity and technology. It emerges that while current federated systems satisfy user needs by allowing the construction of multiple digital data sets, the fragments of which are moored to a central identifier, they fail to provide the user with control over the capability to act in the 'hatch', 'match' and 'dispatch' phases of the digital identity lifecycle. Ultimately, this reduces the user's trust in providers and results in reluctance to disclose personal details.*

*Keywords: Identity, Identity Management Systems, User Needs.*

# 1 INTRODUCTION

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. Supported by multiple organizations, federated systems allow an individual to use the same user name, password or other personal identification to sign on to the networks of more than one enterprise. In order to provide seamless access across technologies and services, federated systems have been introduced. Identity and the ensuing entitlements are then portable across domains (Clarke 2004). For service providers, the key issues concern authentication of identity and single sign-on to one or multiple organizations. This enables relevant business processes, ensures privacy and security, and facilitates the assignment of access rights, privileges and synchronisation of changes to these things over time (Gengler 2004). Examples include Liberty Alliance, MS Passport, Ping Identity and Web Services Federation.

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. Other benefits include the enabling of service providers to easily and securely provision accounts and provide access privileges, and finally, 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). In a fragmented digital world, it can be seen that 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, even the body of research that critically examines organisations' attempts to federate peoples' digital identities, provides few insights into what users themselves really want.

The aim of the research reported in this paper is to address this gap by exploring user perceptions of identity and identity management systems. The research involved two phases. The first phase is a detailed analysis of the literature. Six key issues in relation to digital identity are revealed. The second phase involved an empirical study of end users. The analysis of the data revealed two key user needs which are discussed with critical reference to the ability of federated systems to align with user requirements.

The final section of the paper discusses the potential of federated digital identity management systems to meet user needs in light of changing digital environments.

## 2 IDENTITY AND IDENTITY MANAGEMENT

### 2.1 Human Identity

Human identity is the individuality and personality of a particular person and may be characterised by a number of properties of that person (Simpson and Weiner 1989). The properties of an individual may be intrinsic (eg. DNA, retina scan, hair colour), descriptive (eg. name, birthplace), demographic (eg. occupation, gender), geographic (eg. address, country, postcode) or psychographic (eg. interests,

preferences). The identity of a person denotes that person, reflecting their uniqueness, and provides a means of differentiating them from others. It also provides a means of establishing similarity with others in various roles (eg. customer, employee) and social groups (eg. elderly citizens, family) (Carroll and Murphy 2004).

Identity encompasses all the essential characteristics that make each human unique but also all the characteristics that enable membership to a particular group or culture as well as established status within the group (Roussos et al. 2003). The identity of a person comprises a large number of personal properties. All subsets of the properties represent partial identities of the person and may relate to roles the person plays. Depending on the context, the person may have multiple different partial identities (Claub and Kohntopp 2001).

Roussos et al. (2003) offer three principles of identity:

#### *The Locality Principle*

Identities are situated within particular contexts, roles, relationships and communities. People will have multiple different and overlapping identities in different contexts, and each of these should be respected. A global or universal identifier makes little sense.

#### *The Reciprocity Principle*

In human relationships, knowledge of identities is negotiated and both sides in the relationship should know how properties that characterise identity are exchanged and used. Relationships should be symmetrical and reciprocal.

#### *The Understanding Principle*

Identity serves as a basis for understanding in two-way relationships. Mutual knowledge of identities improves the ability to see things from the other point of view and leads to trusting relationships.

## **2.2 Digital Identity**

The networked environment in which we live and work requires digital identity – it is the key by which we are able to communicate, interact, transact, share reputations and create trusted relationships with people, business and devices electronically. Roussos et al. (2003) note that digital identity is the electronic representation of personal information of an individual or organization (name, address, phone numbers, demographics etc.) To cater for the increasing complexity and sophistication of computing systems and infrastructure, identity management providers have extended this definition to include ‘resources’ which may be machines or other entities capable of communication.

Turkle (1995) provides an additional perspective, noting that while there is a strong correlation between real life and digital identity, digital identity breaks from the constraints of everyday life allowing users to transcend the limits of the real world. She notes that digital environments allow users to shed the human qualities of age, gender, race, disability and even, as in the case of an HIV positive man who had promiscuous online sex, disease.

The transcendent properties of digital identities are best embodied by the phenomena of MUDS (multi user dungeons) that are networked, online communities. They are similar to massive multi-player games where each player assumes a character, yet their defining feature is that there is no game play involved. A MUD is not goal oriented and there is no notion of winning or success. Users inhabit them purely for the experience of creating a new digital identity (Curtis 1992). “In one MUD a user can be a knight, in another, the user can be a stripper and still in another the same user can be furry genderless bunny (Reid 2004).” Exploring the pleasure users get from playing and experimenting with digital identity challenges the often held notion that digital identity should be thought of in terms of the restriction of information or anonymity

## 2.3 Identity Management

Identity management systems aim to provide access and privileges to end users via authentication schemes (Clarke 2001). For service providers the key issues concern authentication of identity, single sign-on (i.e. one login) to one or multiple organizations to enable relevant business processes, privacy and security matters, assignment of access rights and privileges and synchronisation of changes to these things over time.

Secure identity management systems provide sophisticated exemplars of the integration or federation of data, information and services from both the 'supply side' or service providers and 'demand side' or end users (Clarke 2004). Federation of identity refers to emerging standards and specifications for single sign-on, linked access to multiple computer systems and manipulation of accounts and information across different organizations. Successful federation on the 'supply side' rests on the adoption of a common standard (currently two standards are emerging, the Liberty Alliance consortium and the Microsoft/IBM Web Services Federation) and a degree of trust within and between providers and users. Federated identity has been aided by loosely coupled web services architecture based on XML (Extensible Markup Language) and SOAP (Simple Object Access Protocol) standards. This proposes communicating identity data through a mix of federation standards and simple end user web services programming using a distributed technical architecture. This is a more flexible and widely adopted model than pure use of standards in a complete systems integration project.

Access to data and services needs to be managed and depends on who the user is, or on some attribute(s) of the user. The process comprises three phases (Clarke 2004):

1. Pre-authentication      Registration or enrolment and some level of assurance that the person is who they claim to be – “who is the person that I am going to associate with the identifier?”
2. Authentication            Provide confidence that the user is the person who was intended to use the particular identifier
3. Authorisation            Establish privileges or permissions to the user – “what access should I permit this user?”

Before the Internet, organizations performed these identity management functions themselves. There is a strong move to have them now performed by third party organizations – initially by IT companies, then consumer marketing companies, governments and mobile phone companies. An early example is Microsoft Passport which enables single sign-on to multiple Microsoft sites and other organizations (based on user consent).

Identity management may be seen from the “supply-side” – governments, organizations and information technology vendors, or the “demand-side” – customers and citizens. Identity management systems need to find a balance between the sometimes conflicting requirements of these two stakeholder groups.

## 2.4 Key Issues with Identity Management

### 2.4.1 Control and Power

The creation and management of information about individuals is central to identity management. Although organizations in the private and public sector cannot exchange such information without the user's consent, permission is often given without the user's specific knowledge. For example, the disclaimer that states information will be passed on is often hidden in the fine print. A possible solution is to have interlinked record-keeping (identity management) systems to monitor the exchange of information. A second solution is to use different digital pseudonyms with each organization. This

is because pseudonyms cannot be linked - meaning users stay in control. Users can then protect themselves against organizations sharing their digital details.

Clarke (2004) claims that the true benefits of federated systems are largely for the provider, in that organizations and governments gain valuable information while the user's privacy is being compromised by the compilation and circulation of detailed user profiles. However, as Hagel and Rayport (2000) point out, it can be argued that the implications of this are that federated systems essentially represent a trade off, where the user sacrifices privacy and control over personal information for the ease and convenience that one consolidated digital identity brings. They argue that a solution to this is that consumers should capitalise on this situation and demand value in exchange for information.

#### *2.4.2 Authentication*

Authentication in general is a process by which confidence in some assertion is gained. eBusiness depends on the reliability of a range of assertion type statements, sometimes about identity and often involving value or attributes. Risk assessments can help organizations to clarify what assertions are most in need of authentication. Many transactions can be carried out anonymously or pseudonymously. Nyms can be used for persistent communication and profiles can be associated with them. Identity management systems frequently assume that the identity provider knows the identity behind the nym, and the identity provider assigns the nym – a very limited implementation of nyms. Clarke (2004) notes that because pre-authentication is very weak, many schemes support pseudonymity by default and sometimes anonymity. They are accidentally privacy friendly.

#### *2.4.3 Trust*

Identity management is important for building trust relationships; however, the growth of electronic commerce has been hindered by a lack of trust between consumers and service providers (Roussos et al. 2003). A major reason for this is federated identity management systems provide users with limited options to control and personalise their data. Without a sense of control, or the ability to personalise, users become reluctant to reveal details about themselves, instead preferring to provide as little information as possible (Clarke 2004). This is a problem for providers and organizations as detailed information about the user is a valuable asset. A possible means of fostering greater trust would be if providers were to both give users an element of control over aspects of their digital identity and the security measures to protect it. This would give users the opportunity to personalise their digital identity and decide what they revealed in relation to the context of the activity.

#### *Security*

Identity theft often occurs when personal information is used by someone else without their knowledge. It usually supports criminal activity, including fraud, deception, or obtaining benefits and services in the person's name. Identity theft is the fastest growing type of electronic crime and it is expected to accelerate (Roussos et al. 2003). It is particularly prevalent in the digital domain because all that is needed is one piece of information about that person, for example, a credit card number, to steal their identity. Recent examples of this are the ChoicePoint where thieves stole identity information from over 140,000 individuals without breaching or hacking into the company's network and Lexus Nexus where data on over 300,000 people was stolen. It would appear that neither legislation nor private company security measures are able to keep pace with the technology used to gather and organise identity data.

As well as theft, there are also non-malicious breaches of security due to poorly designed systems, processes and governance. It is primarily the responsibility of organisations to guard against these types of breaches.

#### 2.4.4 Privacy

Privacy relates to the claims of individuals that information about themselves should generally not be available to other individuals or organizations, and where data is possessed by another party, the individuals must be able to exercise a substantial degree of control over that data and its use (Koch and Worndl 2001, p4). Organisations generally use notices of consent or disclosure to make statements about privacy. Empirical studies show that Internet users are very concerned about their privacy are not inclined to provide personal information when requested – they want more anonymous transactions (Koch and Worndl 2001, p4). A balance is required between effective governance, legal needs and national security needs on the one hand, and individual dignity and privacy on the other hand (Clarke 2004). This should include organisations making their privacy notices as clear and transparent as possible.

Privacy is also influenced by culture and cultural differences may dictate different privacy requirements in different countries. For example, the European Union has a unique set of privacy requirements in relation to the use of electronic data that is different to that in the United States.

#### 2.4.5 Multiple Identities

Clarke (2001) argues identity has a multi-faceted quality, therefore, reducing rich and complex user information into a single digital entity results in systems that fail to capture the intricacies of everyday user behaviour. This was supported by Roussos et al (2003). They argue that identities are situated within particular roles, relationships and communities and that people will have multiple, different and overlapping identities in different contexts. Each of these should be respected, thus, a global or universal identifier makes little sense. This means there is a strong need by people to have many identities and avoid their federation. “Silos are good, at least for privacy” (Clarke 2004, p41). On the other hand, where ‘context’ is viewed from a technical standpoint incorporating attributes such as physical location, device type and network, a global identifier with multiple attributes makes sense to protect identities. Privacy and security requirements vary depending whether a user is located within a wired secure office network, versus a less secure wireless home environment versus an unsecured internet café. For the device, there may be different levels of identification required for a PC versus a wireless laptop versus an internet phone. For the network, there are varying security requirements dependent on dial-up, versus GSM versus CDMA access. Standards such as Liberty Alliance and PingId, acknowledge that people need multiple identities but still maintain the idea of an underlying single, federated identity – a global set of attributes from all a person’s existing accounts. Multiple identities are assumed to be a problem for individuals and federation will be of benefit. It may help in some circumstances but will certainly improve the social control interests of business and government.

### 3 RESEARCH DESIGN

As discussed above, the first phase of the research involved a detailed analysis of the literature that revealed six key issues. The second phase involved an empirical study using a mix of open-ended interviews, focus groups and cultural probes. The findings reported on in this paper are restricted to the results of the analysis of the open-ended interviews. The open-ended interviews were semi-structured and used a protocol based on the six key issues identified previously. Participants were recruited using an agency and were paid for their participation. They were each young professionals who used information technology intensively in their jobs. A total of ten interviews, each of approximately one hour duration were conducted. The interviews were audio taped and later transcribed into digital text. The text was then introduced into N6, a computer program for the analysis

Comment [s1]:

of qualitative data. N6 was used to aid in the management of the data during coding – the start of the process through which the transcripts were searched for emerging themes.

The data was analysed using the qualitative technique of grounded theory (Strauss 1997). This meant that we did not set out to test a hypothesis; rather the data was examined to uncover what theory best accounted for the emerging themes. Initially, the six key areas that were pinpointed in the literature review were employed as a lens through which to interpret the findings. Analysis at this level provided a useful overview of the users' perceptions of digital identity management systems; however, understanding the data at this level alone was insufficient. For example, finding out that 10 out of the 10 users expected their data to be protected in terms of privacy, or that nine out of 10 users wanted the majority of their transactions to be anonymous, provided little insight into users' real needs. Furthermore, there were many contradictory responses that indicated further investigation of the data was needed. For example, all of the participants reported the need for separate multiple identities while at the same time, nine of the 10 users indicated that they desired the benefits of a federated data set. In keeping with Strauss's approach, the next level of analysis explored the relationships between the emerging themes. This enabled a deeper understanding of the empirical data and ultimately led to discovery. The result was the identification of two user needs.

## **4 EMERGING THEMES**

In this section we will explain how two separate, yet interrelated user needs emerged from the study. The description of each user need will be accompanied by a critical assessment that explores the ability of federated identity management systems to align with each of the user requirements.

- 1) The need for multiple digital data sets that are moored to a central identifier.
- 2) The need for control over these data sets.

### **4.1 Users Need Multiple Data Sets that are Moored to a Central Identifier**

The literature review revealed that an integral part of human identity is that it is neither singular nor static; rather we take on different roles depending on the context of the activity (Claube and Kohntopp, 2001). A key theme to emerge from the user study was that this is not only true for real life identity, but extends into the digital world. User 245 (each participant is denoted by a unique three digit identifier) noted that when she was younger she created the identity "little miss tiger" for online chat sessions, while user 243 explained, "you can fool the digital world by putting forth different information, for example you can have a hotmail address that actually isn't your name. While none of the participants in the study actively participated in the extreme re-creation of identity that, as discussed in the previous section, characterises MUD interaction, user 245 emphasised the importance of being able to experiment creatively with the expression of digital identity, noting her 'little miss tiger' identity was blonde, 23 and bore little resemblance to the 16 year old teenager she was at the time.

User 250 noted that in everyday life, the segregation of identities acts as a self-protection mechanism. "I tend to compartmentalise my life quite a lot and that way if something goes wrong with one segment, it doesn't necessarily have to overlap, whereas it used to all be bundled up together." In the same way that multiple identities provided protection in the real world, so too did this apply in the digital world, notably, the use of multiple identities provided users with a sense of security over their personal information. User 247 noted, "I separate or compartmentalise my personal information when I don't know the source of who is asking for them." While user 245 exhibited concerns that if all information is kept under one banner it could be accessed by the wrong person.

Multiple identities were an important part of the users' experience in digital environments, however, for the participants in the study, they did not 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. It could be seen that multiple digital data sets should not be thought of as disembodied entities, but as part of the cohesive whole that forms the meta-identity of the person. As user 243 noted, having a hotmail address for social activities and a work email address is just as natural as handing out a business card in a work context or using a married name in a family environment. Even when using pseudonyms, users still see digital incarnations as a being firmly grounded to a central identifier. User 244 noted, "to me, (the use of pseudonyms) is not another identity..." The need to have separated information that is part of centralised meta identity was also noted by user 245: "I combine them so that it is easier for me to understand in terms of keeping it all together". As discussed previously, users fragmented their information in terms of security, however, even in this context there was still the need to have the information originate from one place. For example, 246 kept several email accounts for security reasons yet all of them originated from the one email client - hotmail.

The emergence of the user need for multiple data sets that are firmly moored to a central identifier goes against the trend of the literature that theorises about the effect of federation from the users point of view. Clarke (2004) and Roussos et al (2003) for example, argue that federated systems fail users by discouraging the fragmentation of information and forcing users into a situation where they must provide personal details that are not only kept in one place, but managed by a third party. However, what the literature fails to capture, but was evident in the study, is that while users initially profess an ideological opposition to organizations compiling data about them, in practice, they are actually quite blasé about revealing information. After stressing the need for providers to respect the privacy of information, user 244 paused to factor in the cohesion that federated identity management systems brought to his day-to-day life. He then modified his stance, noting, "Well at the end of the day as long as I don't get someone knocking on my door, I am not too fussed about what they do with the information". User 251 was also typical of users in the study, initially reporting the need for separate digital identities "it is fairly important to segregate identities" while later in the interview expressing a desire for the benefits of federation.

"I could have a blanket agreement with one organization to say that you are free to hold my information but then to release the information to other third parties – its almost like saying you are my agent and therefore if you want to release that to anybody else that's fine but please come to me and ask for my authorisation and tell me what it is about."

What then, are the possibilities for identity management systems to align with user needs? Clarke, (2001) points out, that from an organisational or business perspective, multiple identities are assumed to be problematic. Yet, he notes, that this does not mean federated models need to be rejected. As noted in the literature review, many standards, for example Liberty Alliance and PingId, acknowledge that people need multiple identities but still maintain the idea of an underlying single, federated identity – a global set of attributes drawn from the collective of a person's existing accounts. Federated systems have the potential to allow users to express multiple digital identities while at the same time, mooring the fragments to a central identifier. When thought of in light of the user need for a diversity of data sets that are still part of a complete 'meta-identity', federated systems seems ideally suited to meet this need. However, as user 250 stressed, the willingness to supply information and the desire for federation, quickly evaporates when the user loses control over it.

Another aspect to this is the users trust in an organisation. This is related to their perception of risk in sharing their information with an organisation which is in turn related to the perceived brand and reputation. For example, a person may be comfortable with their reputable insurance company linked to their bank, but not so with a Hotmail account linked to the same bank.

## 4.2 Users need Control over their Data

The participants willingness to provide personal information, and furthermore, their desire to federate, challenged commonly held perceptions that the advantages of federated identity management systems are purely for the provider. The previous section revealed that users quickly overcame their ideological objections to providers and organizations compiling detailed profiles in return for the perceived benefit of having cohesion amongst fragmented data sets. This section however, reveals that despite potential benefits, users are considerably less likely to disclose information if they loose control. User 244 noted that she “wouldn’t be too fussed about revealing personal information provided I have control, because the whole world works like that.” While user 245 typified participants in general when she said her concern was not with providing information but in the inability of systems to allow her to maintain control over the data. “I don’t mind giving out information that is going to benefit me in some way, but I do want to control it...(User 245)”

Establishing precisely what aspects of control users want is complex and requires further empirical research. Our data hinted at the different types of control users required at different phases of the digital identity lifecycle. We will discuss control in relation to three broad and overlapping phases – ‘hatch’, ‘match’ and ‘dispatch’.

*Hatch:* digital identities are born, or evolve, and our participants expressed strong views on the role that they desired in that creation process, and the relationship that the digital identity should have with their ‘real’ or non-digital identities.

*Match:* digital identities, especially when federated, are networked collations of identifying and related information. The emergent properties of these information networks include more thorough and complete pictures of end users than many are comfortable with. Our participants wish to have a clear voice in the organization of the identity networks.

*Dispatch:* In time digital identities become obsolete, or their continuance is undesirable for some reason. Our participants expressed feelings of powerlessness in their ability to ‘kill off’ a digital self.

### 4.2.1 *Hatch*

Users need to ‘hatch’ a digital identity that contains data that is relevant to ever changing real life identity. User 243 noted that she did not mind organizations keeping records of her personal details such as her drivers license information, health insurance and bank details, further more, with trusted partners, she had no objections to this information being shared. Rather, she resented that she could not access her data to update details such as change of address. She wanted her digital identity to be a continually accurate representation of her current state and her inability to control this was a major concern. This was in keeping with Chaum who as far back as 1985 noted that users are losing control over the accuracy of their digital identity:

Computerisation is robbing individuals of the ability to monitor and control the ways information about them is used. As organizations in both the private and the public sectors routinely exchange such information, individuals have no way of knowing if the information is accurate, obsolete, or otherwise inappropriate (Chaum 1985, p1030).

Furthermore, as user 243 pointed out, in order for data to be accurate, it must be compiled from information users had provided themselves. “I am in control of what others know about me when I am the one providing them the information. I lack control of what others know about me when they obtain information from other areas, other than from me directly.” Yet as user 247 noted, providing and updating digital information about one’s self is problematic because users can’t always access, or know how to access, their details. “I couldn’t update it (my personal information) because I actually

didn't know the source, so I couldn't go there and update it or take it out and that really annoyed me, but I couldn't do anything about it...I feel vulnerable when people take the information away from me and store it somewhere else."

The study revealed that if providers of digital identity management services are to align with user needs, they need to supply end users with the ability to act in the 'hatch' phase of the digital identity management cycle. This translates into the need for systems that facilitate digital identities that are compiled by information users themselves have provided and where the information about the person is accessible so it can be updated by them, thus ensuring the digital data sets remain accurate. Clarke (2001) notes the nature of federated identity management systems are such that they offer a 'synchronisation of change'. This means once information about a user has been updated, the changes are applied to all the information about that person. In this way the structure of federated systems are well positioned to meet this. The issue then, lies with the willingness of the provider and organization to allow users access to their data.

#### 4.2.2 *Match*

Koch and Worndl (2002) argue for digital identity management systems that "allow people to define different identities, roles, associate personal data to it, and decide whom to give data and when to act anonymously" (Koch and Worndl 2001, p2). This was a strong theme to emerge from the study. User 251 for example, highlighted the subtleties of choice that drove disclosure, noting he used the technique of divulging highly personal information to business colleagues in order to create better relationships. It can be seen that while computers can compile information about a person, in many situations, computers cannot decide what information about the user is appropriate to reveal in the context of a specific activity or interaction. This drastically reduces the occasions where service providers can act on behalf of the user.

In order to overcome the inability of systems to supply the correct information for the context of the interaction, activity or context, users need to be given control over the capability to act at the 'match' phase of the digital identity management lifecycle. The study revealed this amounts to three degrees of disclosure.

- 1) Highly compartmentalised data sets
- 2) Minimum disclosure (anonymity)
- 3) Detailed, personalised composites.

1) The compartmentalisation of information allowed users to associate the correct information to the relevant data. These boundaries were an integral part of the mechanisms users put in place to ensure efficient digital identity management. The prevalent divisions were between social, professional and personal identities. User 244 noted "I separate or compartmentalise my personal information when I feel the need to keep my part of my personal life separate to my work, or my social life". User 246 supported this. "My (homepage) address is not for business, it's personal, for fun."

From the users' perspective, compartmentalisation occurred as a natural extension of the different roles we play in everyday life. From the providers perspective this practice indicates a need to capitalise on the ability of federated systems to facilitate the division of information. It should be noted however, that while the need for these divisions was a recurring theme for all the participants in the study, the level of compartmentalisation offered by federated models was not sufficient for all users. User 250 physically segregated the different aspect of her life by assigning each digital identity its own artefact – one laptop for work and a separate laptop for her personal and social activities.

2) Participants in the study revealed an important characteristic of digital environments is that they allow them to eliminate features of their identity that they do not want to reveal. User 249 likened the need for digital anonymity to the need to walk down the street without telling each person you encountered your personal details. The strong desire to restrict information, was however, accompanied by awareness that absolute anonymity is difficult to achieve. "...you are never

anonymous, it's just a level of how much information they can gather about you" (User 244). At best, users aimed for a 'perceived' anonymity, a digital identity that disclosed as little as possible or pseudonymity, an alternative identity that was not immediately associated with their personal details such as name and address. As user 247 noted, "I will try to create a fictitious name to be anonymous".

The need for anonymity, or 'perceived' anonymity, is one that federated systems are well suited to meet. For example, anonymity can be permitted in a federated identity situation if the user is given the power to suppress personal details when they choose. Anonymity can also be achieved in the context that the use of a single identifier allows interactions in digital environments that reveal little or none of the person's real life identity. Nyms can be used to achieve pseudonymity, with information being recorded about a person that is only revealed in certain situations.

3) The desire for anonymity was contrasted by the need for digital identities that revealed highly personalized information with users indicating digital disclosure can become more meaningful when elements of non-digital identity are incorporated. For example, 246 noted that while her homepage restricted information such as her address, date of birth and age, she took particular pleasure in maintaining a site reflecting her interests and hobbies, taste in music, star sign and opinions in general. Conversely, user 247 noted that the experience of having a university email address that consisted only of numbers was disconcerting. A digital identity that was reduced to a series of numbers was not only problematic for her own sense of identity, it complicated the process by which she recognised the identity of incoming mail from fellow students, who were also operating under an email address that revealed none of their real life identity.

The user need to augment basic digital data with information that provides clues to what the person is like in real life is significant and challenges the traditional function of federated digital identity management systems as mechanisms whose primary role, as Clarke (2001) notes, is to ensure security. The data from the study indicated that a shift in focus is necessary and calls for the emphasis on restricting information to be opened up to include a focus on what is revealed. As user 249 stated: It is funny because we were talking about our privacy and the way we don't want our information out, but as a business person I want my information out and the more out as possible (User 249).

Other roles for digital identity such as facilitating convergence and lowering the cost of transactions to both organisations and individuals need to be taken into account.

Facilitating the process through which users compartmentalise, restrict and personalise information, poses an obvious challenge for providers. Attempts to design a system that meets these user needs are further complicated by the fact that these different modes of disclosure do not occur as separate phenomena, rather, they happen simultaneously. For example, user 246's desire for a web page that provided an in-depth account of her taste and opinions was accompanied by the need for her address, date of birth and age to be suppressed.

#### 4.2.3 *Dispatch*

Lack of control was a concern for users in terms of what happens to their information once it had been dispatched. Participants in the study described that once they revealed information about themselves they had little or no control over the information, who gets access to it and for what purposes it is used. Significantly, this does not mean that users are reluctant to supply their information to trusted companies like banks. Rather, a major concern was the ability to know who the trusted parties in turn were supplying information to and how it would be used. For example, user 244 noted that a major concern with providing information was that once disclosed, was always 'out there'. As mentioned in the section on hatching digital identities, this meant information often became inaccurate. However, a further concern for users was that the data could be stored and used well beyond the life cycle that the user intended the information to have. User 251 noted that information he provided about himself at a much earlier date, had been passed on and ultimately came back to haunt him in the guise of unwanted spam mail.

It got to the point where I was getting over 100 emails a day of just rubbish. It was like getting 100 Bunnings and Kmart and \$2 shop catalogues a day, every single day and you have to empty it out and throw it in the bin and of course you just don't have time, no one has time in their day to read all these things.

As another example, user 243 as a respectable 50 year old school teacher may well want to retire or destroy the 'little miss tiger' identity. The power to kill off an obsolete or unwanted digital identity is so important because it completes the digital identity lifecycle. Just as federated systems provide users with the ability to maintain the relevance of a digital data set through the use of synchronisation in the hatch phase, ideally, synchronisation could facilitate the process through which a user could kill off a redundant digital identity in one go.

#### 4.3 Summary

In summary, it can be seen federated digital identity management systems are well positioned to facilitate the first user need for multiple data sets that are moored to a central identifier. Yet, there is still an overriding barrier to user participation with federated systems and that is a perceived lack of control over information, specifically, the capability to act at the 'hatch, match and dispatch' phases of the digital identity lifecycle. This is where the possibility for federated systems to align with user needs becomes more sophisticated. However, it was clear that this is a challenge that providers need to meet. As user 251 noted, federated information, without control, was akin to "a cesspool sitting somewhere on the internet that says this is who I am".

## 5 CONCLUSION

"We have a life based on technology, so giving access to everything is basically handing over your life." This poignant observation made by user 247 highlights the opportunities and responsibilities that face not only providers and organisations but also designers and administrators of identity management systems.

The study revealed that federated systems potentially have real relevance for users who, it can be seen, are increasingly willing to supply information and even sacrifice their privacy if they are given the capability to 'take charge' of their digital self. However, failure to provide control results in the erosion of trust between the users and the provider and culminates in a culture of use where the user aims to suppress rather than reveal information. This means more than a failure to meet user needs. Not only is detailed information about the user a valuable asset (Hagel and Rayport, 2000) the growth of electronic commerce has been hindered by a lack of trust between consumers and service providers (Roussos et al (2003). Ultimately, failure to provide control represents a loss for providers and organisations themselves.

## References

- Carroll, J. and Murphy, J. (2004) Who am I? I am Me! Identity Management in a Networked World, Proc 4th International We-B Conference, Edith Cowen University, November
- Cham, D. (1985) Security Without Identification: Transaction Systems to make Big Brother Obsolete, Communications of the ACM, 28:10 (October), 1030-1044
- Clarke, R. (2001) Authentication: A Sufficiently Rich Model to Enable e-Business, Xamax Consultancy., (accessed 6 June 2004)  
<http://www.anu.edu.au/people/Roger.Clarke/EC/AuthModel.html>
- Clarke, R. (2004) Identity Management, Xamax Consultancy
- Claube, S. and Kohntopp, M. (2001) Identity Management and its support of multilateral security, Computer Networks, 37, pp 205-219

- Curtis, P. Mudding: Social Phenomena in Text-Based Virtual Realities (1992) (accessed 10<sup>th</sup> July 2005) <http://citeseer.ist.psu.edu/curtis92mudding.html>
- Gengler, B. Standard ID clears a path in password jungle, IT Alive Section, The Australian, August 3rd 2004, p 4
- Hagel, J. and Rayport, J. (2000) The Coming Battle for Customer Information, Harvard Business Review, January-February, pp 53-65
- Koch, M. and Worndl, W. (2001) Community Support and Identity Management, Proc. European Conference on Computer Supported cooperative Work, Bonn, Germany (September)
- Liberty Alliance Project (2003) Introduction to the Liberty Alliance Identity Architecture, Revision 1.0, March (accessed 5 August 2004)  
<https://www.projectliberty.org/resources/whitepapers/LAP%20Identity%20Architecture%20Whitepaper%20Final.pdf>
- Reid, E. (2004) Cultural Formations in Text-Based Virtual Realities. Cypersociology Magazine. January 28
- Roussos, G., Peterson, D. and Patel, U. (2003) Mobile Identity Management: An Enacted View, International Journal of Electronic Commerce, 8:1, pp 81-100
- Simpson, J.A. and Weiner, E.S.C. (1998) *The Oxford English Dictionary*, Clarendon Press, Oxford.
- Strauss, L., and Corbin, J. (1997). *Grounded Theory in Practice*. Sage,
- Turkle, S. (1995). *Life on the screen: Identity in the age of the Internet*. New York: Simon & Schuster.