Behaviour & Information Technology
Vol. 30, No. 1, January–February 2011, 51–62

Taylor & Francis
Taylor & Francis Group

Identity crisis: user perspectives on multiplicity and control in federated identity management

C. Satchell[a]*, G. Shanks[a], S. Howard[a,b] and J. Murphy[c]

[a]*The University of Melbourne, Parkville, 3010, Australia;* [b]*Department of Computer Science, Aalborg University, Aalborg, Denmark;* [c]*Novell Pty Ltd, Australia*

(*Received July 2006; final version received February 2008*)

Federated identity management systems synthesise complex and fragmented user information into a single entity. Literature from the provider's perspective notes 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 are the perceptions of federation from the user's perspective. This study reports an empirical user study that examines the relationship between identity and technology using contextual interviews, focus groups and cultural probes. It emerges that while current federated systems satisfy user needs by allowing the construction of multiple digital data sets that 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. To provide seamless access across technologies and services, federated systems have been introduced. Supported by multiple organisations, they allow identity and the ensuing entitlements to be portable across domains (Clarke 2004). For service providers, the key issues concern authentication of identity and single sign-on to one or multiple organisations. 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 of federated identity management frameworks include Liberty Alliance, Ping Identity, MS Cardspace and Web Services Federation. More recently, user-centric federated identity management frameworks, including Higgins (Eclipse Foundation 2006) and PRIME (Leenes *et al.* 2007), have been proposed.

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 is extended to the end user. Furthermore, he notes the other cited benefits are largely from the business perspective and asks why the customer should 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 people's digital identities provides few insights into what users themselves really want.

The aim of the research reported in this study is to address this gap by exploring user perceptions of identity and identity management systems. The research involved two phases. The first phase was a detailed analysis of the literature. Six key issues in

*Corresponding author. Email: satc@unimelb.edu.au

ISSN 0144-929X print/ISSN 1362-3001 online

DOI: 10.1080/01449290801987292
http://www.informaworld.com

relation to digital identity were revealed. The second phase was an empirical study of end users. It involved three different data gathering methods: open-ended interviews, focus groups and cultural probes. 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 study discusses the potential of federated digital identity management systems to meet user needs identified in the study.

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 1998). The properties of an individual may be intrinsic (e.g. DNA, retina scan, hair colour), descriptive (e.g. name, birthplace), demographic (e.g. occupation, gender), geographic (e.g. address, country, postcode) or psychographic (e.g. interests, preferences). The identity of a person denotes that person, reflecting their uniqueness and providing a means of differentiating them from others. It also provides a means of establishing similarity with others in various roles (e.g. customer, employee) and social groups (e.g. elderly citizens, family) (Clarke 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 (Clauss and Koehntopp 2001).

Roussos *et al.* (2003) offer three principles of identity: locality, reciprocity and understanding. The locality principle argues that 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. 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. Furthermore, 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.

These three principles provide a context for the concept of digital identity and help us to understand some of the requirements for successful digital identity and the limitations of identity management systems.

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 organisation (name, address, phone numbers, demographics, etc.)

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 phenomenon 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 a 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 include processes, policies and technologies that 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 organisations 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 organisations. 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, organisations performed these identity management functions themselves. There is a strong move to have them now performed by third party organisations – initially by IT companies, then consumer marketing companies, governments and mobile phone companies. Several federated identity management frameworks have been proposed (for example Higgins (Liberty Allicance 2003, Eclipse Foundation 2006) and PRIME (Leenes *et al*. 2007)) that should provide a foundation for future systems.

Identity management may be seen from the 'supply side' – governments, organisations 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.

There are several types of identity management: centralised, federated and user-centric. Centralised identity management systems (for example Microsoft Passport) have one central definition for digital identities that is shared amongst partners. Federated identity management systems rely on partners to authenticate their respective users and each vouch for their access to services. User-centric identity management systems enable users rather than partner organisations to maintain control of their digital identities (see Jøsang *et al*. (2007) for a useful discussion of types of identity management system).

3. Key issues with identity management

A critical analysis of literature revealed a number of key issues with identity management. These include control and power, authentication, trust, security, privacy and multiple identities. Each of these is now discussed, linked to relevant literature and provides a basis for data collection in the empirical study.

3.1. Control and power

The creation and management of information about individuals is central to identity management. Although organisations in the private and public sector should not 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 organisation, enabling users rather than organisations to stay in control of their digital identities. Users can then protect themselves against organisations sharing their digital details.

Clarke (2004) claims that the true benefits of federated systems are largely for the provider, in that organisations 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.

3.2. Authentication

Authentication in general is a process by which confidence in some assertion is gained – it need not relate to identity in particular. eBusiness depends on the reliability of a range of assertion type statements, sometimes about identity but often involving value or attributes. Risk assessments would help organisations to clarify what assertions are most in need of authentication. For some transactions there is a need to know the 'identity' of the other party – for very few transactions there is a further need to know the 'entity' or the real-world thing (Clarke 2004).

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 person's 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.

3.3. Trust

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 that 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 organisations as detailed information about the user is a valuable asset. A possible means of fostering greater trust would be if providers were to give users an element of control over aspects of their digital identity. This would give users the opportunity to personalise their digital identity and decide what they revealed in relation to the context of the activity.

3.4. Security

Identity theft 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, Identity Theft Task Force 2007). It is particularly prevalent in the digital domain because all that is needed is one piece of information about a person, for example a credit card number, to steal their identity. Stronger authentication mechanisms, for example the use of biometrics, can help to reduce the prevalence of identity theft.

3.5. Privacy

Privacy relates to the claims of individuals that information about themselves should generally not be available to other individuals or organisations, 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 Woerndl 2001). Empirical studies show that Internet users are very concerned about their privacy and are not inclined to provide personal information when requested – they want more anonymous transactions (Koch and Woerndl 2001). 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).

3.6. 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). 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 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.

4. Research design

The aim of the research is to explore user perceptions of identity and identity management systems. The research design consisted of two main phases. The first phase of the research comprised a detailed analysis of the literature that revealed six key issues, discussed previously. The second phase involved an empirical study. A mixed method approach was decided upon that included ten open-ended, one-on-one interviews, two focus groups with five users in each group and a cultural probes study conducted with the five participants from one of the focus groups. The use of these three disparate methods ensured that data was collected in both a laboratory setting (semi-structured interviews and focus groups) and in the context of the daily life of the participants (cultural probes and related interviews). This enabled the collection of a rich set of data and triangulation of the data across the different methods.

The interviews were semi-structured to ensure that data collected was highly relevant and focused on user needs in identity management systems while at the same time permitting participants to elaborate on issues that emerged during the interview (Neuman 2003). The interview protocol was based around the six key issues discussed previously together with two scenarios to provoke comment. 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 10 interviews, each of approximately 1 hour duration were conducted.

The focus groups were designed to further explore user needs in identity management systems by facilitating discussion amongst participants to encourage development of opinions by interaction between participants (Krueger 1988). The focus groups used the same interview protocols as the semi-structured interviews and involved the same participants split into two groups of five.

The interviews and focus groups were audio taped and later transcribed into digital text. The text was then introduced into N6, a computer program for the analysis 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. Once the themes had been identified, they were placed into a matrix.

Cultural probes (Gaver *et al.* 1999, Vetere *et al.* 2005) are useful when the phenomena under study are difficult to access, or likely to be radically changed in the process of their examination. In addition to the *post-hoc* interviews, and focus groups, we deployed cultural probes to provide the participants with an opportunity to 'reflect in the moment' on their perceptions, needs and, importantly, future desires. Rather than containing reliable and valid information on the current practices of our participants, the value of the probe packs came in their facility to trigger creative reflection and capture inspirational fragments. The probe packs consisted of a diary, a scrapbook, a camera, and various other items including pens and scissors. Postcards, return email addresses and sms/text numbers were provided so that the participants could contact the researchers at any moment. The probe data, consisting largely of diary and scrapbook entries and associated interview notes, were filtered for identity related issues and observations, and these instances were used as a tertiary data source.

We have chosen to keep these three data sets (interviews, focus group findings and cultural probe returns) distinctive in our reporting in this study, as we wish to highlight the distinguishing features of the three approaches. We therefore will refer to the interviewees as I#, the focus group participants as FG#, and the cultural probe returns as CP#.

5. Analysing the data sets

5.1. The interview data

The interview data was examined first (Satchell *et al.* 2006). The transcripts were analysed using the qualitative technique of grounded theory (Strauss and Corbin 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 lenses 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 in the interviews 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:

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

The interview process was the most useful when a participant had an in-depth understanding of the technology in relation to their own needs and could provide articulate and informed feedback. However, there were instances when a participant would seem unsure of how the questions being posed might relate to their own experiences. As will be discussed in the next section, the focus groups helped overcome this problem.

5.2. *The focus group data*

The focus groups added value with the presence of multiple participants helping users share their experiences more readily than many did in the one-on-one interview environment. Furthermore, the participants provided narratives that would either remind other participants of similar experiences, or provide a perspective from which to express an opposing opinion. For example, focus group participant FG2a rejected the idea that a federated digital identity management system could successfully compile personal preferences or be of assistance when conducting online activities. This user maintained that a real-life identity is far too malleable to be translated into a digital snapshot of the person. 'I don't think it [a digital composite] will be any clear indication of the individual, I mean sometimes at lunch you read The Age on the Internet and sometimes you read the Herald Sun…' This statement galvanised another member of the focus group to express an opposing point of view. User FG2b argued that user FG2a was in danger of missing out on the benefits of life in the digital age. Even when pushed about the 'big brother' nature of federated digital identity management systems, user FG2b remained convinced that a synthesised digital representation of tastes and preferences was a positive thing:

> Interviewer: What if they are tracking your preferences in all sorts of activities?.... So you might be walking down the street one day and get some prompting from your mobile device saying that you're right in the area of Kentucky Fried Chicken, how would you feel?
> User FG2b: Kinda handy!

Overall, the focus groups were successful in generating discussion between participants and although no significant new insights emerged from the two sessions, the re-occurrence of the themes from the interviews helped support the initial findings.

5.3. *Cultural probes*

The cultural probe packs lent a new dynamic to the study with users expressing their experiences through fragments of text including diary entries, email exchanges and post it notes, as well as images including Polaroid photos, advertisements and drawings the users produced themselves.

The order in which the data was analysed was done through convenience rather than by design, yet it was beneficial that the cultural probe data be examined last. This was for two reasons. First, a new insight that had been overlooked in the analysis of the interview and focus group data emerged. Second, the perspectives brought by the cultural probe data enhanced the earlier findings.

5.3.1. *Generating new insights*

The emerging themes from the cultural probe data were in keeping with the re-occurring themes from the interviews and focus groups. However, a new insight did emerge. Two out of the five users in the cultural probes study reported that they saw their mobile phones as a highly personalised device. For example, participant CP5 described how her mobile phone was integral to her sense of identity as a participating member of a social network and noted that that her face-to-face social contact had been replaced with mobile mediated interactions (see Figure 1). Furthermore, both of these users revealed that they saw their mobile phones as providing more control, security and privacy over digital identity

Figure 1. Taken from user CP5's scrap book. It was accompanied by the caption 'Sometimes my social life becomes a touch dial. I've recently only communicated with my friends through my phone'.

than any other technology and thus found their mobile phones to be the ideal site to maintain the bits of data that constitute personal digital identity. With this new finding in mind, the previous interview and focus group data was revisited and although it had not been articulated as strongly, five other users supported this notion.

5.3.2. *Enhancing previous findings*

The cultural probe data enhanced the previous findings because it allowed users to draw on references from popular culture to convey the point they are trying to make. This is especially helpful when examining a topic as intangible as digital identity. For example, lack of control over the dissemination of personal details was expressed by user CP6 through the inclusion in their scrap book of the widely circulated email Identity Federation: Making Pizza Delivery More Efficient in 2015 (see Table 1). This email documents the fictitious attempts of a hapless user in the year 2015, whose efforts to order a pizza are thwarted by the operator's extensive knowledge of his current health and financial status.

6. User needs

In this section we will explain how two separate yet interrelated user needs emerged from the interviews, focus groups and cultural probe packs. 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.

6.1. 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 (Clauss and Koehntopp 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. Interviewee I245 (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 interviewee I243 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, interviewee I245 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.

Interviewee I250 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. Interviewee I247 noted, 'I separate or compartmentalise my personal information when I don't know the source of who is asking for them', while interviewee I245 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,

Table 1. An extract from the email Identity Federation: Making Pizza Delivery More Efficient in 2015.

Operator:	"Thank you for calling Pizza Hut"
Customer:	"Hi, I'd like to order."
Operator:	"May I have your NIDN first, sir?"
Customer:	"My National ID Number, yeah, hold on, eh, it's 6102049998-45-54610."
Operator:	"Thank you, Mr. Sheehan. I see you live at 1742 Meadowland Drive, and the phone number's 494-2366. Your office number over at Lincoln Insurance is 745-2302 and your cell number's 266-2566. Which number are you calling from, sir?"
Customer:	"Huh? I'm at home. Where d'ya get all this information?"
Operator:	"We're wired into the system, sir."
Customer:	(Sighs) "Oh, well, I'd like to order a couple of your All-Meat Special pizzas . . ."
Operator:	"I don't think that's a good idea, sir."
Customer:	"Whaddya mean?"
Operator:	"Sir, your medical records indicate that you've got very high blood pressure and extremely high cholesterol. Your National Health Care provider won't allow such an unhealthy choice."

nine participants in the study specifically stated that this 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 interviewee I243 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. Interviewee I244 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 interviewee I245: '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, I246 kept several email accounts for security reasons yet all of them originated from the one email client – hotmail. Finally, interviewee FG1b noted, 'I've got everything in both my phone and my computer and it is both personal and professional – all together and so it definitely becomes a part of my identity'.

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 user's 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 organisations compiling data about them, in practice they are actually quite blasé about revealing information. For example, after stressing the need for providers to respect the privacy of information, interviewee I244 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'. Interviewee I251 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 – it's 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.

Overall, six participants reported an ideological and philosophical aversion to federated identity silos, yet this ideological need for fragmentation was overshadowed by the benefits of integration. Perhaps this is best thought of in light of the wallet metaphor. Every day we carry a purse or wallet where we keep our cards, licence, money and photos together in one place. This is not an ideal situation because if it gets lost it is not only difficult and time consuming to replace the contents, there is a real security risk. Yet, we do it anyway. In this way it can be seen how for users in the study, the ideological concerns for privacy take a back seat to the everyday need for 'ease of use' and 'convenience'.

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 from 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 interviewee I250 stressed, the willingness to supply information and the desire for federation quickly evaporates when the user loses control over it.

6.2. *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 organisations 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 lose control. Interviewee I244 noted that she 'wouldn't be too fussed about revealing personal information provided I have control, because the whole world works like that', while interviewee I245 typified participants in general when she said her concern was not with providing information but with 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...'.

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 organisation 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.

6.2.1. *Hatch*

Users need to 'hatch' a digital identity that contains data that is relevant to ever changing real-life identity. Interviewee I243 noted that she did not mind organisations keeping records of her personal details such as her driver's licence information, health insurance and bank details; furthermore, 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, p. 1030).

Furthermore, as interviewee I243 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 I247 noted, providing and updating digital information about oneself 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 from 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 is well positioned to meet this. The issue, then, lies with the willingness of the provider and organisation to allow users access to their data.

6.2.2. *Match*

Koch and Woerndl (2001) 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 Woerndl 2001). 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.

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. Interviewee I244 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'. Interviewee I246 supported this: 'My [homepage] address is not for business, it's personal, for fun'.

From the user's perspective, compartmentalisation occurred as a natural extension of the different roles we play in everyday life. From the provider's 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. Interviewee I250 physically segregated the different aspects 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' (interviewee I244). 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 interviewee I247 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 personalised information with users indicating digital disclosure can become more meaningful when elements of non-digital identity are incorporated. For example, I246 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, interviewee I247 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 in necessary and calls for the emphasis on restricting information to be opened up to include a focus on what is revealed. As interviewee I249 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 as much out as possible'.

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, I246'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.

6.2.3. 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, I244 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 lifecycle that the user intended the information to have. Interviewee I251 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.

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.

7. Discussion

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. 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 Craigslist (Craigslist is a centralised network of online urban communities, featuring free classified advertisements) (Heardt 2005). It can be seen that great opportunities exist for federated identity management systems because they offer users more than silos of information. They offer the potential for much needed synthesis of previously fragmented data sets, or what Roussos *et al.* (2003) note as the first principle of identity – multiple, different and overlapping identities in different contexts.

Despite the benefits, 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 the at the 'hatch, match and dispatch' phases of the digital identity lifecycle. 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'.

The possibility for federated systems to align with this second user need represents a challenge providers need to meet. Although there is no one, simple solution, the data suggests user perceptions of control are influenced by the technology itself. Specifically, the mobile artefact was seen by seven users in the study to provide a great degree of security, personalisation and privacy. Although more research is needed to see why this is the case, the study indicates the mobile phone engenders perceptions of security and trust because it is seen as a personal belonging that always accompanies the person and thus is a more natural and trusted means of conveying the user's identity.

With greater convergence comes greater opportunity for providers to capitalise on the values and philosophies embedded in the mobile device. This does not necessarily indicate the mobile phone should become central to federated digital identity management systems. Rather, that the values attributed to it should be embedded into systems that provide users with control of their own information and consequently digital identities that no longer exist in some remote data base, but rather embedded in the person's personal technology as a natural extension of the user.

8. 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.

Further research is needed to establish how the needs of providers might align with these needs and desires of the users.

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. Furthermore, even when users exhibit an ideological opposition to the information about themselves being compiled into single composite, the data revealed that most users are fundamentally lazy and this overrides their need for privacy. 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.

As Roussos *et al*. (2003) note in their second and third principle of identity, both sides must be involved in the process through which identities are characterised, exchanged and used. Only then can trust be engendered. This is important from the provider's perspective because 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, improvement in the ability to provide user control will represent a significant gain for both the supply and demand sides of the identity management relationship.

Acknowledgements

Thanks to all the participants in the empirical study and to Elizabeth Hartnell-Young for her assistance with the data collection. This work is part of a broader research programme involving chief investigators S. Howard, J. Carroll and G. Shanks, and is supported on behalf of Novell by J. Murphy. The research is funded by the Australian Research Council and Novell through Linkage Project LP0347459 'Humanising the Convergence of ICTs'.

References

Chaum, D., 1985. Security without identification: transaction systems to make big brother obsolete. *Communications of the ACM*, 28, 1030–1044.

Clarke, R., 2001. *Authentication: a sufficiently rich model to enable e-business* [online]. Xamax Consultancy. Available from: http://www.anu.edu.au/people/Roger.Clarke/EC/AuthModel.html [Accessed 6 June 2004].

Clarke, R., 2004. *Identity Management*, Xamax Consultancy.

Clauss, S. and Koehntopp, M., 2001. Identity management and its support of multilateral security. *Computer Networks*, 37, 205–219.

Curtis, P., 1992. *Mudding: social phenomena in text-based virtual realities* [online]. Available from: http://citeseer.ist.psu.edu/curtis92mudding.html [Accessed 10 July 2005].

Eclipse Foundation, 2006. *Introduction to Higgins* [online]. Available from: http://wiki.eclipse.org/index.php/Introduction_to_Higgins [Accessed 5 July 2007].

Gaver, B., Dunne, T., and Pacenti, E., 1999. Design: cultural probes. *Interactions*, 6, 21–29.

Gengler, B., 2004. Standard ID clears a path in password jungle, IT Alive Section, *The Australian*, p. 4.

Hagel, J. and Rayport, J., 2000. The coming battle for customer information. *Harvard Business Review*, 75, 53–65.

Heardt, D., 2005. Web 2.0 high order bit – identity 2.0 [online]. Available from: http://identity20.com/media/WEB2_2005 [Accessed 15 September 2006].

Identity theft task force, 2007. Combating identity theft: a strategic plan, United States of America Federal Trade Commission report [online]. Available from: http://www.identitytheft.gov/reports/StrategicPlan.pdf [Accessed 6 July 2007].

Jøsang, A., Alzomai, M., and Suriadi, S., 2007. Usability and privacy in identity management architectures. *In*: *Proceedings of Australasian Information Security Workshop (AISW'07)*, Ballarat, Australia, January [online]. Available from: http://sky.fit.qut.edu.au/~josang/papers/JAS2007-AISW.pdf [Accessed 5 Feb 2008].

Koch, M. and Woerndl, W., 2001. Community support and identity management. *In*: *Proceedings of European Conference on Computer Supported Cooperative Work*, Bonn, Germany: Kluwer Academic Publishers, September, 319–338.

Krueger, R.A., 1988. *Focus groups: a practical guide for applied research*. Newbury Park, CA: Sage Publications.

Leenes, R., Schallabock, J., and Hansen, M., 2007. PRIME white paper v2, version 1.0 [online]. Available from: https://www.prime-project.eu/prime_products/whitepaper/ [Accessed 5 July 2007].

Liberty Alliance Project, 2003. Introduction to the Liberty Alliance Identity Architecture, Revision 1.0, Marc [online]. Available from: https://www.projectliberty.org/liberty/content/view/full/183/(offset)/15 [Accessed 5 August 2004].

Neuman, W.L., 2003. *Social research methods: qualitative and quantitative approaches*. Boston: Allyn and Bacon.

Reid, E., 2004. Cypersociology Magazine, January 28 [online]. Available from: http://www.cybersociology.com/files/5_theborg.html [Accessed 12 December 2005].

Roussos, G., Peterson, D., and Patel, U., 2003. Mobile identity management: an enacted view. *International Journal of Electronic Commerce*, 8, 81–100.

Satchell, C., *et al*., 2006. Knowing me, knowing you: end user perceptions of identity management systems. *In*: *Proceedings European Conference on Information Systems*, Gothenburg, June, CD-ROM, p. 12.

Simpson, J.A. and Weiner, E.S.C., 1998. *The Oxford English Dictionary*. Oxford: Clarendon Press.

Strauss, L. and Corbin, J., 1997. *Grounded theory in practice*. Thousand Oaks: Sage.

Turkle, S., 1995. *Life on the screen: identity in the age of the internet*. New York: Simon & Schuster.

Vetere, F., *et al*., 2005. Mediating intimacy: designing technologies to support strong-tie relationships. *In*: *Proceedings of ACM*, CHI, Portland, Oregon, USA, pp. 909–912.