

The Privacy of Money and Health: A User Study

Associate Professor Supriya Singh
Dr Kylie Cassar Bartolo

Royal Melbourne Institute of Technology and Smart Internet Technology Cooperative Research Centre
Melbourne, Vic, Australia
Email: supriya.singh@rmit.edu.au

Royal Melbourne Institute of Technology and Smart Internet Technology Cooperative Research Centre
Melbourne, Vic, Australia
Email: kylie.bartolo@rmit.edu.au

Abstract

In this paper we report on a qualitative and quantitative study of people's control of personal information in Australia. User control is the central requirement for privacy and identity. Control of personal information varies according to activity and social context. Boundaries of privacy differ for money and health. The challenge for design is to digitally replicate these multifarious interpretations of privacy and identity while ensuring ease of use.

Keywords

Money, Health, Privacy, Identity, User study, Information

INTRODUCTION

There have been few user studies concentrating on how people want to control personal information and manage their identities while engaged in different activities. Existing policy studies for the main part focus on attitudes to privacy rather than behaviour in activity contexts (see Federal Privacy Commissioner 2000). In much of computer science and engineering literature – and in some science fiction – the ultimate horror is that of stolen identity. In everyday language, this equates to the ultimate crime of annihilation (See Lambert 2002, Saunders 1999, Vinge 2001). Identity fraud is primarily a security issue, and is spoken of in the language of defence. Become as anonymous as possible, withhold personal details, and it will be more difficult to steal your identity. Hence the coming together of identity and anonymity. The two concepts are also linked through the legal understanding of privacy current since the late 19th century, that is "the right to be let alone" (Woo 2001).

Our qualitative and quantitative study of users' control of personal information and identity adds a needed perspective in two ways. First, it focuses on activities. Second, it shows that user control of information can mean control of sharing information. Privacy does not always translate to anonymity. We draw on literature in sociology and social psychology for our understandings of privacy and identity. In much psychological and social science literature, identity is seen more in terms of the construction of different versions of the self, depending on context (see Altman 1975, 1977, Kroger 2000). In our work we have also drawn on the postmodern approach to a multiplicity of identities (Turkle 1995) and the ethnographic approach of a continuity of identity between the real and virtual worlds (Miller and Slater 2000).

This user study has been conducted specifically to input into the design of mobile technologies in the Smart Internet Technology Cooperative Research Centre (SITCRC), which brings together universities, industry partners and governments¹. More generally, the concepts of "privacy", "identity" and "control" cut across the use of all information and communication technologies, and hence are a core concern of SITCRC.

¹ The SITCRC brings together 12 Australian universities and three significant corporate partners. The research program comprises four technical streams focusing on smart personal agents, natural adaptive user interface, intelligent environment and smart virtual networks. The User Environment Program overlays these technical streams to ensure the user is at the centre of the design from the very beginning. The aim is to develop useful and commercialisable technologies. Hence in SITCRC, we work at the intersections of the social, technological and business perspectives.

In this paper we focus on the qualitative and quantitative findings on the privacy of money and health. These findings yield the core requirement of users' control of the sharing of their personal information. We describe the users' perspective informing the user study. In the next section we discuss how people see money and health as two of the most private areas in personal communication. Privacy however means controlling what you say about yourself in different contexts and to different sets of people. People share their health information more broadly with family and friends, compared with money. With health, quality of care depends on sharing information that is as complete as possible with the health professional. The desire is for shared control of health information between the health professional and the patient. The picture is different with money, for people assert control over most money activities by giving as little information as possible to the financial institution. We go on to show that the use of electronic money enhances fears about a loss of privacy because of insecure channels. The patient – health professional relationship however is still mainly face-to-face. The emphasis is on care and context, rather than technology. In the concluding section we dwell on the central importance of users' control of information for their perception of privacy and versions of identity. The challenge for design is to digitally replicate these different interpretations of privacy and identity while ensuring ease of use. The issue for business strategy is to gain customers by giving them control of their own information.

THE USER STUDY

In our Australian user study of the control of personal information, we have placed users and their activities at the centre, within the social and cultural context (Singh 2001). The users' perspective shares much with "activity theory" and its emphasis on a "web of activities" (Bertelsen and Bødker 2003) rather than assume a linear, sequential structure. We also draw on studies of the social shaping of technology (MacKenzie and Wajcman 1999) to investigate how technologies shape and are shaped by social relations and cultural values.

Hence in the user study, we focus on people's attitudes and behaviour in relation to privacy and identity in the digital and non-digital worlds, emphasizing the meaning and use of communication channels. We discover how people present and manage their identities by controlling the kind and extent of information they share with people at different points in their "circle of care".

The qualitative study

The user study comprises a qualitative study of 17 persons in Melbourne and a quantitative study of 1010 persons in Launceston Broadband Project, Tasmania. The qualitative study was a "grounded study" (Strauss and Corbin 1990) where we moved from the data to emerging theory. We conducted open-ended interviews with a convenience sample from our personal and professional networks between Dec 2003 and March 2004.

The sample included men and women from different educational backgrounds and occupations. The people interviewed covered a wide age spectrum. Half the people interviewed were Anglo-Celtic in ancestry, the other half being people from other backgrounds.

The interviews were conducted by four researchers, including the authors. We worked with an agreed interview guide, that served as a checklist of the issues we wanted to cover. The interview guide was updated as the result of previous interviews and analysis. The interviews covered demographic data and their use of technologies at work and at home. The central part of the interview focused on activities. We asked about the kind of information they comfortably gave about themselves in the context of payments and banking; entertainment; personal communication and social networks; health and education. We probed further for the people with whom they shared their information about these activities and the communication channels they used. We then asked them to tell us of occasions when they felt they were in control of their personal information, and instances when they felt uncomfortable because of a loss of control.

As we began to hear ambiguities in the concepts of privacy, identity, and security, we modified our interview guide to ask people towards the end of the interview to give us their definition or version of these concepts.

We analysed the data using N6, a computer program for qualitative analysis. We sorted the data first in broad nodes so that we could catch differences in the coding of data. Using matrices and memos, we identified emerging themes. We went back to N6 to check for negative cases. We used the personal voice to write up our data and themes, acknowledging agency and the researcher's role in the gathering and analysis of data.

The quantitative study

The quantitative study was an online survey of 1010 persons conducted by Telstra in the Launceston Broadband Project² (Fabre and Robbins 2004). The survey was administered between March and May 2004.

The survey helped us understand attitudes and behaviour towards personal information among broadband users. It is not representative of the Australian population nor adult Australians who use the Internet at home. Women were under-represented in the survey when compared to Internet users at home, as Table 1 makes clear. The survey was also not representative for age. There was an under-representation in the 18-34 group, with the other age groups over-represented. In this initial round of analysis, we are keeping this lack of representativeness in mind, when we deal with gender and age.

Gender	Australian population 18 years and over %	Australia % of Internet users 18 years and over at home, 2002	Survey sample %
Male	49	52.9	75
Female	51	45.8	25

Sources: ABS 2003, Fabre and Robbins 2004

Table 1: Gender in the survey sample

Age	Australia % of population 18 years and over, 2002	Australia % of Internet users 18 years and over at home, 2002	Survey sample %
18-24	13.1	17.4	6
25-34	20.0	24.2	16.2
35-44	20.2	25.9	28.4
45-54	18.2	19.1	26.1
55-64	13.0	9.7	11.7
65+	15.4	3.6	5.0

Sources: ABS 2003, Fabre and Robbins 2004

Table 2: Age in the survey sample

The questionnaire was designed keeping the user at the centre, building on preliminary insights of the qualitative study. Hence the focus was on understanding how people control their personal information according to the activity context, audience and channel. The survey questions included:

- Please indicate which of the following information/activities you consider to be private (eg Your health information; Information about your assets; Information about your debts; Your income; Digital photographs of you and close family or friends; Sexual preferences....)
- With whom would you share your personal health information (e.g., pregnant, back pain, asthma)? (Share with Partner; Share with No One; Share with Close friends; Share with Anyone; Share with Work Colleagues; Share with Family members)
- With whom would you share information about your salary or income? (Share with Partner; Share with No One; Share with Close friends; Share with Anyone; Share with Work Colleagues; Share with Family members)

² Members of the Launceston Broadband Project participate in various surveys as part of research promoting ADSL services, in exchange for concessions to the cost of broadband access to their home/businesses. The Launceston Based Project has over 1800 members made up of people from the Business community (25%) and consumer /household base (75%). Members of the business community were invited to participate as consumers rather than as business leaders.

- Please rank from most to least, the form of communication, which you would reserve for personal/private information (Internet; mobile phone; fixed phone; Internet with encryption; Face to face)

MONEY AND HEALTH ARE INTENSELY PRIVATE

Both the qualitative and quantitative studies showed that people saw money and health as the most private areas of personal communication. So in this paper we concentrate on money and health. After money and health, sexual preferences, personal digital photographs and life events were seen as most private (See Table 3). Respondents were given the choice between the responses: Private and Non-private

No.	Please indicate which of the following information/activities you consider to be private	Percentage who regard it as private N=1010
1.	Information about assets	96
2.	Information about debts	94.7
3.	Health information	93.7
4.	Income	93.1
5.	Sexual preferences	89.9
6.	Digital photos of you and family/friends	85.8
7.	Life events	78.9
8.	home address	68.6
9.	Work or academic performance	64.0
10.	Your hobbies or interests	45.2
11.	Your occupation	43.0
12.	Your name	39.8
13.	Your thoughts, feelings and opinions	13.6

Source: Fabre and Robbins 2004

Table 3: Privacy of personal information

The qualitative study was equally definite about the privacy of money and health. Salary, bonuses, savings, assets, debts are private. Having them disclosed without your choice could lead to a loss of money or an inappropriate presentation of self. This is true for all our interviewees except one. Harriet, 18, who is just moving into employment, but is still living at home, did not see money as private. She is more concerned about over-spending and protecting information about her love life. The remaining 16 saw money as private, across all ages, gender, income groupings and ethnicity. The privacy of personal money is so entrenched in Australia that even when there is little money involved, the principle of privacy is accepted. Even Amy, 22, working casually and travelling, who does not have “copious amounts of money”, sees money and banking as private.

Fifteen of the 17 people interviewed talked of health information as private and were concerned about the consequences of an inappropriate sharing of health information. Inappropriate disclosure of health information was seen to have a serious impact in terms of work and personal life. The only exceptions were Cathy, 29, a genetic counsellor and Harriet who did not overtly speak of the privacy of health information. However, Cathy in her professional work was very conscious that health information was private. Harriet did not mention health information in her definition of personal information. The privacy of health was true across age, gender, and ethnicity. It also applied for the three health professionals in the study. It was true whether a person had a chronic disease or not.

Health and money are private in different ways. We summarise these differences in table 4. In the following sections we detail these differences.

Characteristics of privacy	Money	Health
Boundaries for sharing information	Focused nearly wholly on the partner	Wider boundaries that include family and friends
Minimisation of risk	Withholding information	Sharing more information to increase the quality of health care
Control of information	A person is in control of his/her financial information.	Health professionals are central to the construction of health information
Consequences of breach of privacy	Could lead to loss of money	Could lead to discrimination
Use of technology	Electronic money is well established for users	Health is not technology-mediated for users

Table 4: Privacy of money and health

BOUNDARIES OF DISCLOSURE

Privacy means controlling what you say about yourself in different contexts and to whom. It is this expression of self that often has privacy being seen as synonymous with identity. However, identity is constructed and presented from both public and private information. The difference between privacy and identity needs to be stressed, for in technological and business writings, there is at times an implicit assumption that a person has a single identity, and that this identity can be managed or controlled. Control is the common link between privacy and identity. It is in the loss of control that there is a loss of privacy. One's sense of self and identity are threatened.

In this section we show the contextual aspect of privacy by showing that people choose to discuss their health more broadly than money with family, friends and work colleagues. We illustrate this by choosing the most critical aspects of money and health (See Table 5).

Boundaries of sharing	Critical Information Money (eg Debts)	Critical Information Health (eg cancer)
Share with Partner	83.5%	88.7%
Share with Family members	27.9%	77.7%
Share with Close friends	11.0%	53.5%
Share with No One	9.6%	3.9%
Share with Work Colleagues	1.3%	13.7%
Share with Anyone	0.8%	2.1%

Source: Fabre and Robbins 2004

Table 5: Money is shared more narrowly than health

Money is private but people talk about it with people within "their circle of care". This circle in Australia always includes the partner and sometimes is confined to the marital unit. The centrality of the marital unit differs across cultures, but in Australia the marital unit is the main domestic financial unit (Singh 1997). However as our qualitative study shows, the boundaries of privacy about money are wider than the partner. They include one or more parents, maybe adult children, siblings and close friends, who are of the same socio-economic status.

Health information is shared more freely than information about money with partners, family members and close friends. Intimate others need to know this information so that they can provide support at times of ill-health.

Controlling the sharing of information is crucial. When this control gets taken away, then as Tom's story shows, there is discomfort and trust is shattered. Tom, an electrical engineer in his mid-forties, describes a time

when his wife shared information about his reproductive health with her friends without his consent. He says, "I'm sometimes not ready to share things with her, because I know it will get broadcasted, or it could get broadcasted...So it's out of my control, whereas if I speak to...other people.. it's under my control".

Where a person feels he or she has this control, they may choose to go beyond their own circles and share the information with the wider community. Becky, 58, a health professional, who had breast cancer, says, "I set up a web page about breast cancer to help other people...because when I went looking for information on breast cancer on a personal level I didn't find very much...If I can help one other person by discussing it openly with them, then I would be more inclined to be very open."

This open sharing is remarkable, for people find it difficult to speak about pain and suffering. Talking of illness can evoke feelings of shame and discomfort, especially in social settings. Becky in her professional life protects the privacy of patients. But for her own health issues, as she is in control, she is ready to share information that may be useful.

CONTROL OF INFORMATION

In this section we focus on the different ways control is interpreted in money and health. A person exercises control over money by giving sufficient information for the transaction and withholding other pieces of related information. It is the way control is exercised with money that is often seen as the template for privacy. With health however, quality of care depends on sharing information that is as complete as possible with the health professional. In cases of mobility or where several health providers are involved, there is the desire for shared control of health information between the health professional and the patient.

We show how these different interpretations of control relate to the nature of financial and health information. With money activities such as payments, people tend to separate different kinds of money according to origin and use. Hence they separate wages from bonuses; grocery money from inheritance (Singh 1997). This separation of monies means there is separation of information about money. Users own their financial information and may choose to withhold or disclose it for payments transactions.

In health, it is the health professional who owns the information. Patient knowledge becomes health information (e.g., symptoms) only when it goes through a health professional (e.g., health record). Hence most people choose to share knowledge with the health professional, but want some measure of control themselves. Traditionally this diagnosis and associated information are controlled by health professionals. Patients in many countries, including Australia, have the right to access their health information. The Internet is aiding patient's knowledge so that the questions can be more targeted. Better communication and partnership between patients and health professionals is also becoming the accepted ideal in the field (Teutsch 2003). However, health information policy have been slow to respond to these changes.

Restricting information about money

One of the common themes in the qualitative study is that control over money is exercised by withholding information. This is done in the physical and digital worlds. Fatima, 39, a teacher shares information about money with her sisters, mainly because they do not ask her questions. When faced with direct questions about her salary in her new school in Melbourne, she refused to answer. She says, "I find that's very personal, because I don't ask such questions. Throughout my years of teaching I haven't asked anyone how much they are getting in their salary." When people persist with their questions, she tells them, "It's based on your teaching experience. You can go to the website and check the salary scales." Fatima says it is a sensitive issue and can "rip" a friendship. "I respect... other people's privacy, so I expect them to respect (mine)."

Becky also refused to answer when she thought people were trying to extract information from her. She will share information about money with family and close friends, as long as she is directly asked and has the choice to disclose or not to disclose. But when she and her husband bought a new unit near the city, she was asked questions that went around in a circle. People would say "Oh, it's very expensive to live in (this area), isn't it?" She would answer, "Oh, not too bad." Or they would say "That would have cost you a pretty penny". She'd say, "Oh no, not too bad." "It is like a tease", she noted. On her own though, she told her close friends with ease.

In our qualitative study, none of the participants sought Internet anonymity. They wanted transparency about the organisation's need for the financial information. Becky wondered why organisations who sell her things online need so much personal detail, which is unrelated to the fulfilment of the transaction. Moreover the insecurity of digital channels exposes her to a breach of privacy. Like others, she has responded at times by giving different versions of her name. Her doubts about the security of her personal information were confirmed when spam came to that particular version of her name.

Professional mediation of health information

In contrast to family, friendship circles and community contexts, the patient-service provider relationship is the only one where there is no reservation about sharing health information. The reason for sharing is to facilitate medical care. However people in the qualitative study spoke of the control of health information in different ways, particularly when they did not have a constant relationship with their health providers, or when they were away from their usual place of residence. Digital records with the patient, despite their privacy implications, were discussed as potential technological solutions.

The preferred option is for the patient and the health provider to have control of the health information. This was borne out in the quantitative data. The present situation in Australia of health providers being the main controllers of information, was the least preferred option as seen in the table 6.

Who should have control over your personal health information?	Percentage
You alone	33.4
You and your health provider	65.7
Your health provider alone	0.8

Source: Fabre and Robbins 2004

Table 6: Control over personal health information

CONTROL OF INFORMATION ON THE INTERNET

The need for control becomes greater on the Internet, for most people see it as insecure. In the quantitative study, 47 per cent saw the Internet as insecure and 13.9 per cent saw it as neither secure nor insecure. Where the Internet offers greater relative value and an acceptable risk, people choose to use the channel as Table 7 shows.

Please indicate HOW you MOSTLY pay for your purchases	Face to Face	Using a telephone or mobile phone	Using the Internet
I pay my bank (e.g., mortgage, loan instalments)	30.3%	9.7%	60.0%
I pay my utility bills	24.8%	26.2%	49.0%
I pay for shares	41.9%	14.8%	43.4%
I pay my insurance bills	30.7%	27.1%	42.2%

Source: Fabre and Robbins 2004

Table 7: Payment channels and activities

In the qualitative user study we asked about identity fraud. Only one of the users – Sandra, 38, a finance professional - said she worried about it. Three – Donna, Fatima, Tom – said they were not concerned. Donna, 45, a health professional said she was sure that identity theft could “create havoc... (but) I’m more likely to be struck by lightning or die of cancer or get hit by a bus... The chance of it happening is miniscule...” The other 13 users did not mention it.

Identity theft was also not an experience for 89 per cent of the people in the quantitative study. The greater fear for consumers is their loss of control over their personal information, once they have given it to an organisation. As Hoffman et al (Hoffman et al. 1999) have noted, consumers and providers are united in their desire for more security. However consumers worry that they lose “secondary control” of their information once it is given on the Internet. This is because organisations often prefer the “opt-out” model – that is people have to say they do not want their personal information shared. It is also the case that few organisations tell how they will be using consumer information.

The Internet does not figure highly in discussions of health relationships. The Internet is a channel of information rather than a transactional medium. This is because health is an area mainly based on interpersonal communication. Communication between the patient and the health professional is not driven by technology. Context and human relationships were central. Face to face communication was most important as table 8 shows.

When using more than one health care provider how should personal health information be shared?	Percentage
Face-to-face	76.5%
Using the telephone	37.2%
Print - fax/post	30.4%
E-mail	19.5%
Smart card	22.5%

Source: Fabre and Robbins 2004

Table 8: Channel for sharing personal health information with multiple health providers

CONCLUSION: IMPLICATIONS FOR DESIGN, BUSINESS STRATEGY AND POLICY

In this paper we are reporting on the “discovery” stage of user-centred design (Singh et al. 2003), where initial understandings about privacy, control and identity drawn from the user study are being discussed with business partners and technologists for their implications for design and business strategy. In the SITCRC, because we work in a mixed academic and corporate context, we have been able to delve in greater depth into the issues of privacy than may have been possible in a corporation. We are now at the stage of seeing how the user study translates into user requirements.

This stage of “discovery UCD” is important for one of the major contributions of this study is that it re-frames the core concepts of privacy and identity. The users’ perspective shifts the debate on privacy from a focus on security and anonymity to one of trust and user control. It also illustrates the importance of seeing privacy in the context of activities, questioning the more generalised attitudes to privacy.

This change in the approach to key concepts needs to be workshopped and accepted by the technologists and the business partners in the design team. This is before we can begin to discuss the merits of one design over another. Hence it is in the workshopping of ideas that the major challenges for design and business emerge. In the sub-sections below we discuss the two main points of tension.

Sharing of information vs withholding information

Our study shows that privacy lies in the control of personal information, rather than anonymity or withholding personal information. The emphasis is on controlling the sharing of information. This is a point most often missed in the literature. It is important, for control is most often demonstrated in the boundaries of shared information. The control of boundaries differs according to the activity and social context.

The challenge for design is to digitally replicate these multifarious interpretations of privacy and identity while ensuring ease of use. As Ackerman (2002) says, it is difficult to bridge the “socio-technical gap”. This is “the great divide between what we know we must support socially and what we can support technically” (Ackerman 2002, p. 303). He goes on to say “...There are no current HCI mechanisms to straightforwardly mechanize the naturally occurring, everyday social activity of handling personal information in its entirety. ” (p. 309)

User control vs identity management

In business literature, identity and privacy are often seen as synonymous. Conceptions of identity management are varied (Crompton 2004), but there is the underlying assumption that control of a customer’s demographic information and transactional history will enable the business to “manage” the customer’s identity. A person’s identity is thus linked to one set of personal data.

In health policy, the challenges are equally great. Policy publications regarding health privacy traditionally emphasise protecting information from unwanted third parties and enhancing patient consent. More recently, patient access to their information became another key point of emphasis (Federal Privacy Act 1988, Federal Privacy Commissioner 2002, Federal Privacy Commissioner 2001a, Federal Privacy Commissioner 2001b). There is however a lack of empirical understanding of ordinary consumers’ experiences around the management of personal health information. Our study showed the importance of sharing rather than withholding health information. This emphasis on sharing information has not yet been facilitated in health policy or health information management systems.

Our study shows that once a person does not have control over his or her own personal information and version of self, both privacy and identity are threatened. Identity and personal information are not synonymous, for identity is not always private. There are public aspects to a person’s physical identity, such as appearance and ethnicity. The common factor between privacy and identity is the concept of control. Privacy involves people

controlling their personal information according to context. People also control the way they present themselves, that is their identity.

Our study reinforces literature that emphasises the benefits of consensual privacy (Samarajiva 1997), “social translucence” (Erickson and Kellogg 2002) and recognising consumers’ rights to data ownership on the Internet (Hoffman et al. 1999). But as Hoffman et al. recognise, this way of achieving trust “departs radically from traditional business practice and will be difficult for many companies to implement” (p. 85). The development of privacy rights management, in an obverse form of digital rights management however, may make it technologically possible to track the movement of packets of information. Once this technology is available in the market place, then a company that chooses not to be “translucent” and accountable to its customers, will be sending a negative message.

REFERENCES

- Ackerman, M. S. (2002). The intellectual challenge of CSCW: The gap between social requirements and technical feasibility. In J. M. Carroll (Ed.), *Human-Computer Interaction in the New Millennium* (pp. 303-324). New York: ACM Press.
- Altman, I. (1975) *The Environment and Social Behaviour: Privacy, Personal Space, Territory and Crowding*, Brooks/Cole, Monterey.
- Altman, I. (1977) Privacy Regulation: Culturally Universal or Culturally-specific? *Journal of Social Issues*, 33 (3), 66-84.
- Australian Bureau of Statistics (2003). *Household Use of Information Technology, Australia, 2001-02*. Australian Bureau of Statistics.
[http://www.ausstats.abs.gov.au/ausstats/subscriber.nsf/Lookup/AAD3580B50B6A970CA256D9D00057958/\\$File/81460_2001-02.pdf](http://www.ausstats.abs.gov.au/ausstats/subscriber.nsf/Lookup/AAD3580B50B6A970CA256D9D00057958/$File/81460_2001-02.pdf), Accessed 31 March, 2004
- Bertelsen, O. W. and Bødker, S. (2003). Activity theory. In J. M. Carroll (Ed.), *HCI Models, Theories, and Frameworks: Toward a multidisciplinary science* (pp. 291-356).
- Crompton, M. (2004). *Proof of ID required? Getting Identity Management Right*. Office of the Federal Privacy Commissioner, URL http://www.privacy.gov.au/news/speeches/sp1_04p.pdf, Accessed 20 August 2004
- Erickson, T. and Kellogg, W. A. (2002). Social translucence: Designing systems that support social processes. In J. M. Carroll (Ed.), *Human-Computer Interaction in the New Millennium* (pp. 325-345). New York: ACM Press.
- Fabre, J. and Robbins, J. (2004) *Secure Control of Information: Data Verification and Analyses*. Melbourne, Telstra Research Laboratories
- Federal Privacy Commissioner (2000). Community Attitudes Towards Privacy in Australia, URL <http://www.privacy.gov.au/publications/rcommunity.html>, Accessed 18 June 04
- Federal Privacy Act (1988), URL http://www.privacy.gov.au/publications/privacy88_030504.pdf, Accessed 18 June 04
- Federal Privacy Commissioner (2001). *Health Information and the Privacy Act 1988: A Short Guide for the Private Health Sector*, URL <http://www.privacy.gov.au/publications/hp.html>, Accessed 18 June 04
- Federal Privacy Commissioner (2001b) Guidelines on Privacy in the Health Sector URL http://www.privacy.gov.au/publications/hg_01.html, Accessed 18 June 04
- Federal Privacy Commissioner (2002). *My Health My Privacy My Choice - a Consumer's Guide to Privacy and Health Information*, URL <http://www.privacy.gov.au/publications/chib.html>, Accessed 18 June 04
- Hoffman, D. L. and Novak, T. P. and Peralta, M. (1999) Building consumer trust online, *Association for Computing Machinery. Communications of the ACM*, 42,(4), 80.
- Kroger, J. (2000) *Identity Development: Adolescence Through Adult*, Sage,. Tromsø, Norway.
- Lambert, L. (2002) Asian Underground Banking Scheme: A Field Note, *Journal Of Contemporary Criminal Justice*, 18,(4), 358-369.
- MacKenzie, D. and Wajcman, J. (Eds.). (1999). *The Social Shaping of Technology* (Second ed.). Buckingham, Open University Press.
- Miller, D. and Slater, D. (2000) *The Internet: An ethnographic approach*, Berg, Oxford.

- Saunders, K. M. and Zucker, B. (1999) Counteracting identity fraud in the information age: The Identity Theft and Assumption Deterrence Act, *International Review of Law, Computers & Technology*, 13,(2), 183.
- Singh, S. and Burke, J. and Turner, P. and Castro, M. (2003) *The Discovery Phase of User-Centred Design: Putting Users First in the Design of Smart Internet Technologies*, Paper presented at the The Australasian Conference on Information Systems, Perth.
- Strauss, A. and Corbin, J. (1990) *Basics of qualitative research: Grounded theory procedures and techniques*, Sage Publications, Newbury Park, Calif.
- Teutsch, C. (2003) Patient-doctor communication. *Medical Clinics of North America*. 87 (5), 1115-45.
- Turkle, S. (1995) *Life on the Screen: Identity in the Age of the Internet*, Simon and Schuster., New York.
- Vinge, V. (2001). Introduction. In J. Frenkel (Ed.), True Names and the opening of the cyberspace frontier (pp. 15-23). New York: Tom Doherty Associates
- Woo, J. (2001) *Invasion or giving up of Internet privacy?: A personal divide emerges*, Paper presented at the Pacific Telecommunications Conference, Honolulu.

ACKNOWLEDGEMENTS

We would like to acknowledge the support of our colleagues at the Smart Internet Technology Cooperative Research Centre. In particular, we would like to acknowledge the help of Christine Satchell and John Fabre who had important roles in the qualitative user study. John Fabre and Jessica Robbins conducted the quantitative survey. We would also like to note the importance of the discussions with the leader of the Secure Identity Management Project, John Zic of the University of New South Wales and of John Snare of Adacel.

COPYRIGHT

Supriya Singh and Kylie Cassar Bartolo © 2004. The authors assign to OZCHI and educational and non-profit institutions a non-exclusive licence to use this document for personal use and in courses of instruction provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive licence to OZCHI to publish this document in full in the Conference Papers and Proceedings. Those documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.