The Bank and I: Privacy, Banking and Life Stage

Supriya Singh
Smart Internet Technology Cooperative
Research Centre/RMIT University
GPO Box 2476V, Melbourne, Australia
+61 3 9925 1327
Supriya.singh@rmit.edu.au

Margaret Jackson
Smart Internet Technology Cooperative
Research Centre/RMIT University
GPO Box 2476V, Melbourne, Australia
+ 61 3 9925 5751
margaret.jackson@rmit.edu.au

Jenine Beekhuyzen
Smart Internet Technology Cooperative
Research Centre/Griffith University
Brisbane, Queensland, 4111, Australia
+ 61 7 0405 272068
jenine@griffith.edu.au

Anuja Cabraal
Smart Internet Technology Cooperative
Research Centre/RMIT University
GPO Box 2476V, Melbourne, Australia
+61 3 9925 1576
Anuja.cabraal@rmit.edu.au

ABSTRACT

Enabling customers to influence the way they are represented in the bank's data bases, is one of the major personalization, responsiveness and privacy issues of banking. In this paper we draw on the interim results from a qualitative study of the ways in which Australians think of privacy and money. We find that changes in life stages, residence, and relationships motivate people to share additional personal information with their bank, in order to receive personalized services. We suggest ways how privacy rights management can help customers better represent themselves in a flexible manner reflecting the changes in their lives.

Keywords
Banking, customers, personalization, privacy, privacy rights management

INTRODUCTION

In industrialised countries, the use of electronic money has increased. From the customers' perspective, electronic payments instruments and channels have made money impersonal and virtual. [16]. Seeing the same changes from the organizational point of view, it is the customer who has become impersonal and virtual. As a bank manager said, "I'm actually seeing very, very few of my own... customers… we never see them. We've never even heard of them..." [7, p. 31]. The focus in the bank is then on "some of the intriguing issues of cooperating with 'absent' customers, with cooperating with the 'customer in the machine'"[7, p. 31].

As Hughes et al. say banking technologies help represent this customer 'in the machine'. They say these technologies

> … appear to be routinely deployed as an integral aspect of cooperating with the customer; as a factor in the configuring and reconfiguring of customer behaviour; and as an element in relationship management [7, p. 30].

So from the bank's perspective it is the customer who has become information, with money remaining "real". This is the reverse picture when seen from the users' perspective, where the customer is "real", but the money is virtual.

One of the contributions of our study will be enabling the customer to influence the way the "customer in the machine" is represented. Privacy Rights Management technologies could enable the customer to personalize how he or she wants to be treated by ensuring that the relevant information is included in the way the customer is "configured" within the organization.

In this paper we are reporting on the interim results of a qualitative study on Banking, Personal Communications and Financial Decision Making. This research is part of a wider project focusing on Security, Trust, Identity and Privacy in the Smart Internet Technology Cooperative Research Centre. We are studying these issues from the users' perspective so that users can be central to the design of financial services and bank strategy.

We conducted a qualitative study between April 2005 and March 2006, covering 64 people in Melbourne and Brisbane in Australia. The people were accessed through personal and professional networks. Our sample had:

• 24 men and 40 women. This dominance of women was partially explained because women manage money particularly in the lower income households;

• Three participants aged between 18-24, 20 aged 25-34, 17 aged 35-44, 15 aged 45-54, 7 aged 55-64, and only two aged 65 or over;

• A range of annual household income levels: 14 had an income below $25,000; 13 between $25,000-49,999; eight between $50,000-$74,999, nine between $75,000-

$100,000 and 18 had over $100,000 a year. Two participants did not want to disclose their household income.

• 14 participants had a Certificate or lower educational qualification, 49 had a BA or higher degree and one did not say. Of those who had a BA or higher degree, at least 11 were in IT. This reflected our personal networks also participants' interest in issues of privacy, security and identity.

We chose the qualitative approach for we needed to understand how people manage their financial information across life stages. We also wanted to go beyond attitudes to behavior. The study had at its centre the perspectives of user-centered design where the users' activities within their social and cultural context are at the centre of design [18, 22]. It was a 'grounded' study in that there was a fit between data and emerging theory, rather than a testing of hypotheses [6].

The interviews were transcribed. We used N6, a computer program to assist with qualitative analysis. This meant we first broadly coded the data, then organised the data into matrices to check emerging themes in a transparent manner. We also used the N6 program to identify negative cases so that the study was rigorous. As Morse and Richards [12] say

> The key to rigorous qualitative inquiry is the researcher's ability … of being constantly aware and constantly asking analytic questions of data, which, in turn, constantly address the questions asked. Qualitative inquiry constantly challenges assumptions, constantly challenges the obvious, reveals the hidden and the overt, the implicit and the taken for granted, and shows these in a new light (p. 170).

Once the different facets of money, banking and privacy were understood, these insights were translated to personas and scenarios so that they could be better communicated to bankers on the one hand and on the other hand to computer scientists working on Privacy Rights Management in the Smart Internet Technology Cooperative Research Centre.

PRIVACY, MONEY AND BANKING

Lawyers, technologists, sociologists and psychologists have defined the concept of privacy in different ways. These definitions have little connection with the way people speak about privacy, making it problematic to connect privacy, money and banking.

Different approaches to privacy

Legal debate about the need for a right of privacy is relatively recent, first raised in a seminal article, The Right to Privacy', published in the Harvard Law Review in 1890 [23]. At that time, the issue about privacy concerned intrusions by media and invasions of individuals' rights by government. Warren's family had been hounded by newspaper exposure of private matters

and the Warren and Brandeis paper called for controls on invasion of private and domestic life and the right to protection of the private personality [4].

Later American writers, such as Alan Westin, were to offer different definitions of the concept of personal privacy. Westin adopted a view of personal privacy that was more concerned with control over information about an individual than with intrusions into personal life. This view reflected a growing European debate in the 1960s and 1970s about the protection of personal data, led by organizations such as the Organisation for Economic Co-operation and Development ('the OECD') and the Council of Europe. Westin defined the right of privacy as "the claim of individuals, groups or institutions to determine themselves when, how and to what extent information about them is communicated to others" [24]. This definition has been thought too narrow by some, including Professor William Morison who conducted a review in New South Wales on privacy in 1973, because it excluded people's concerns about intrusions such as unsolicited mail and telephone calls, and intrusive surveillance [11]. Westin's definition arose, however, in the context of the use of new technological methods of recording and disseminating information. The growth of computer technology allowed for the collection, use and disclosure of *personal information* in computer databases, leading to vast amounts of information about people being able to be collected, manipulated and transferred easily. It became possible to capture electronically all the facts that could identify a person in one file.

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 [9, 15, 21]).

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. Anonymity becomes the best way of achieving privacy.

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 [5]. In the user studies on the control of personal information conducted in the Smart Internet Technology CRC, we have found that privacy is seen as the control of the sharing of personal information and control over the representation of ourselves. Privacy did not equate with anonymity. It also did not mean being left alone [17].

This approach to privacy shares much with the literature in sociology and social psychology where identity is seen more in terms of the construction of different versions of the self, depending on context (see [1, 2, 8]. It also connects with the post modern approach to a multiplicity of identities [20] and the ethnographic approach of a

continuity of identity between the real and virtual worlds [10].

Money and privacy

Money is one of the most private aspects of life for Anglo-Celtic couples in Australia. Salary, bonuses, savings, assets, debts are private information. Having them disclosed without your choice could lead to a loss of money or an inappropriate presentation of self. The privacy of personal money is so entrenched in Australia that even when there is little money involved, the principle of privacy is accepted. Money is private but people talk about it with people within "their circle of care". This circle in Australia nearly always includes the partner and sometimes is confined to the marital unit. People also talk about money with one or more parents, maybe adult children, siblings and close friends, who are of the same socioeconomic status [17].

There are important points in a person's life when the privacy boundaries change. There is a greater exchange of money information within the family when there is a need for support. Family support in terms of loans or gifts of money are particularly important for families with a low annual household income (under Aus$50,000). In middle-income families we expect a greater flow of money between parents and children with the rise in housing prices. In Anglo-Celtic Australia, unlike Asia and Africa, money seldom flows from children to parents. This is because of the presence of a welfare net and also because parents pride themselves on their ability to manage. Though money does not get transferred, it is not unusual for children to help manage the financial affairs of their parents, most often of the mother after she has been widowed.

Sharing of information between partners also stops when there is a breakdown in relationship

In our qualitative study people spoke at length about the sharing of information about money. The data substantiated previous qualitative and quantitative studies in the Smart Internet Technology CRC that most people discussed money with their partners. There were exceptions to this general pattern in the following situations:

– In some defacto relationships where the money was separate but equal, there could be little discussion of money.

– When a person had commitments to their natal family or a previous marital family. This was true for blended families, but also true for families where one or both partners were recent migrants and sent money home.

– In families where the husband controlled and managed money.

– In the case of a relationship breakdown.

Not sharing information about money with the partner went together with a pattern of separate rather than joint accounts. It has to be noted that not all separate accounts were accompanied by secrecy. The mix of separate and joint accounts in relationships more often reflected the symbolic meanings of financial independence or jointness, rather than the use of money. Frequently separate accounts were used for joint family expenditure. At times joint accounts were used as a transactional account only by one partner.

Women spoke more about sharing information with parents, some siblings, friends and children. The people we interviewed felt that they spoke about money more openly with their children than was their experience with their own parents.

PRIVACY, SECURITY AND IDENTITY IN BANKING

Issues of privacy in banking spill over to issues of security and identity theft. The common link in the banking context is the risk of losing money via the fraudulent use of the credit card and/or information related to Internet banking..

Though privacy and security were seen as different concepts by our participants who chose to comment, they were increasingly linked in a digital world. A security breach would lead to people having information about you that they are not authorized to have and thus breach privacy as well.

Bridgette, 55-64, (all the names are pseudonyms) an IT academic with a household income of between $75,000 and $99,999, says, she doesn't "have a greatly developed sense of privacy" She says that being on the Internet is not a private activity. And "electronic banking is a way of just stepping outside and shouting to the world". She says,

> I don't care about what people know about me. It wouldn't worry me if people would get onto my bank account online as long as they couldn't do anything with it. If they could then take money out of it, that would worry me.

The people in our sample who commented on banking and privacy were comfortable with the bank knowing copious details about their financial affairs. This was seen as inevitable even though it was the accountant who was the professional with whom money matters were more often discussed. As Ingrid, a PhD student in IT, 35-44, says,

> Privacy I tend to equate more with the information I have allowed the bank in order to do my banking. That is going to be related to actual private details like my name, address, phone number. But it also relates to things like my bank balances, what accounts I have…

She notes "there is nothing private about your dealings with the bank. Everything is reported. Cash transactions are reported. Loans are reported." She thinks the aspect of privacy and banking that is most important is that banks "not …sell my details to marketers"

The privacy issues that did arise for people were more about the bank disclosing details of separate accounts to a person with whom you have a joint account. This disclosure of information was greatly resented. We had two cases of such privacy infringement. In Faroukh's case (45-54 years of age, an IT professional with more than $100,000 in annual household income), the bank showed his wife a separate account that he had with the bank. This was when he and his wife went to visit the branch about their joint home loan. He says he was able to explain it, but felt the bank had not kept his details private.

Identity issues were more connected with credit card fraud and email spam. The issue of identity theft – though of concern – was not something that changed banking behavior or the use of the Internet for our participants. This is different from survey results in the United States where 86 percent of people had changed their behaviour in at least one way because they were concerned someone could steal their identity from personal information on the Internet [14].

The issues of privacy, identity and banking came to the fore mainly for the middle and higher income people. Among the lower income group, the feeling was there was so little money and so there was little to worry about. Only 11 of the 27 people with a household income below $50,000 used the Internet for banking. Hence for most low income persons, issues of Internet and privacy or the wider issues of privacy in a cyber world were not at the centre of their banking.

Privacy, identity, security and the credit card
Issues of money being fraudulently spent with the credit card have been directly experienced by at least three of our 65 participants. Anita, now a housewife, 55-64 with a household income between $55,000 and $74,000 says $AUS 300 was withdrawn from her husband's credit card. When he rang the bank – for he was the primary card holder – the money was returned. This experience left Anita cautious about checking statements and she does not use the credit card on the Internet – choosing to use BPay. However, she regularly uses the Internet to monitor her accounts, transfer money and pay bills. She uses the Internet but worries about the security and keeps a constant eye on her finances. Her only strategy to lessen the risk is that of constant monitoring. She says, "I just hope that… nothing will happen. I just put .. full trust on.. the banks that.. they are doing their best…"

Amber, 28, with a household income below $50,000 says her partner had money taken from his credit card. He rang the bank and they put the money back. This experience of fraud with the credit card and its subsequent solution has gone to enhance the feeling of trust in the bank.

Dora, 35-44, an academic also had a problem with the fraudulent use of her credit card when in South East Asia.

Convenience overrides concerns of security and privacy
Forty-one of our 64 participants currently use Internet banking. Of these 41, two did not routinely use Internet banking. Four were not concerned about the privacy and security, while the other 35 valued convenience over concerns about privacy and security.

Most of the participants, like Anita, were not totally satisfied with the security and privacy of the Internet. Convenience and habit over-rode their concerns. In some cases, they tried not to think of the risks because they could not do much about them. In other cases they used risk minimization strategies such as using credit cards with low limits, using a computer and network they saw as secure, assuring themselves that the site had the sign of a lock to symbolize security.

Ellen, 35-44, an academic in part time work and a household income of over $100,000 says she likes the convenience and the immediacy of the Internet. She buys groceries online and does all her banking on the Internet. She thinks that hackers are going to be able to steal their money one day, "but at this stage I don't see it as a security problem". She tries to be careful by keeping the passwords secure, making sure she is on a secure site. She sees the university server as secure. In the end she tries to stop being anxious by saying nothing is totally secure. And if anything happened she has the confidence to follow up and get the money back.

Laura, 25-34, with her own business in health services, has always banked using the Internet. Replying to questions about trust, privacy and security, she says, "I don't know that I think about it a lot, because I think I don't understand it enough. So I don't think about it. … It's completely hiding your head in the sand."

Others like Gillian, 35-44, a PhD student in IT and a household income of more than $100,000, try and protect themselves by using the latest spyware, or having a credit card with a very low limit. She trusts the bank's system "is secure".

Little you can do about privacy in the cyberworld
Henry, 45-54, an IT academic on a household income of between $75,000 and $99,999 says "In terms of privacy, I don't think we actually have a lot of control over it". The banks have more data on us than we know. He is not sure whether they would sell this data.

> There is an underlying assumption that …there are controls and mechanisms …in place to stop it. .. I am nearly sure most of them aren't there….The only time that you actually find out that there is a huge problem is when it hits you in the arse."

Only ten of the 64 people in our sample read the privacy policy even in a cursory manner. Kevin for instance does not read the privacy policy

…because I know it has more outs than ins…..I know that all that information is shared. Fundamentally, it's all available. Now, whether I read or acknowledge that privacy statement or not, is not going to stop them from making that information available across…institutions.

Peter, 25-34, with a small IT consulting business and a household income of more than $100,000 says the privacy policy is usually a copy of someone else's privacy policy.

Amber, 28, with a household income below $50,000 occasionally reads the privacy policy. She says she is a habitual "checker". Gillian concedes that the privacy policy is important to a certain degree. Ingrid, 35-44, a PhD student in IT, says the privacy policy does not tell what is important. She says,

> Almost every organization will have a privacy policy you have to tick to say that you have read it and understood the conditions, but no-one reads it. The only people that read those kinds of things are people who are new to the Internet, or compulsive people. I don't read them half the time. I tend to be more careful when it comes to things like the financial organizations and I will always scan something to see whether it says we won't sell your details to marketers.

Neither secure nor private

For four participants with a household income above $AUS 50,000, issues of privacy and security are worrying enough for them to not use Internet banking, though they use the Internet and sometimes also buy on the Internet. It is important to note that for the other 19 non-users, 16 had an annual household income of under $A50,000, and three did not find it useful enough.

Callie, 55-64, in accounting with a household income of $50,000 to $74,999 says Internet banking is essentially insecure. She says, no one can guarantee its security. It is not a question of a lack of trust. "I just don't think… you can build a foolproof system." She says,

> I just don't think that organizations are in a position to guarantee … that they've got the safeguards to ensure privacy of information and safeguard it.

Dora, 35-44, an academic with a household income of more than $100,000 says she used Internet banking but stopped after the security breaches reported in the media. She was also worried because she had troubles with her credit card when she was overseas. She says "I just decided that I'd like to know that it was a bit safer before I went back to it."

She continues to occasionally buy tickets and books online but for banking uses the telephone and ATMs. Dora hopes that in five years Internet banking would be more secure so that she can feel comfortable using it. She is naturally risk adverse and in this decision she has been influenced by her husband who is worried about the privacy aspects of online personal information. She is sufficiently worried that she is one of the three who occasionally reads privacy policies.

Alice, 62, a part time teacher, with a household income between $50,000 and $74,999 has used the Internet for work. The most useful part of the Internet for her is to be able to get to the catalogue of the local library. She abhors the Internet, particularly its lack of privacy, while at the same time being enthralled by it. She doesn't use Internet banking and has used telephone banking once when the credit card payment was due, but they were uncomfortable about it. Her husband too feels adamant about not using Internet banking. She at times gives her credit card details over the phone to buy something or sends them off by mail. But in similar situations, her husband sends a check. Media reports of security and privacy breaches seem to confirm their attitude for themselves. They do not consider that the security and privacy situation will ever be comforting enough for them to use the Internet for banking transactions.

Olivia, 25-34, a lecturer in IT and a household income of between $75,000 and $99,999 uses the Internet but does not use Internet banking. She says she is uncomfortable with the idea of her data being used for telemarketing. Moving to security issues she says, "I just feel that my data is not safe." She tolerates banks rather than trusts them. They make mistakes and "are always out to get money off you for fees." The fearful scenario for her is "what if you are putting through a transaction and something happens and it shuts down and then people steal your details…"

Privacy and responsiveness in the bank

In our sample three people saw the bank's use of the Privacy Policy as a way to restrict customer access to information. This was particularly the case with joint accounts, where there was a hierarchical structure of the primary and secondary account or card holder.

Kevin, 45-54, with an annual household income of more than $100,000 says it's a pain "primarily when one or the other has set up the account or done something and we need to change and we're not the original signatory, or were not."

Alice was in a similar situation and felt dismissed as she is not the primary account holder of the joint account. She manages the money but did not bring the account number with her and found the bank would not give it to her. She does not know why she did not give them her credit card. Her husband had to ring up the bank but they said the rules are that only the primary account holder can have particular kinds of information.

Gillian, 35-44, a PhD student in IT, with a household income between $75,000-$99,999 said she and her husband found themselves in the awkward situation where the bank would not accept her changing the contact details for the credit card for both herself and her

husband. She is the one who has the online log-on for the credit card. This is so that they can minimise the number of passwords they have. She says she emailed and asked

> …to change our address, our postal and home address because we had moved. They changed mine but they wouldn't change his, even though I'm a secondary card holder. They said it had to be the primary card holder even though he doesn't have a log-on. So we had to physically ring the bank and change it, which was really not as secure as it could have been.

This meant her husband had to ring the bank to give Gillian permission to change the credit card details. She tried to find out if she could change the details in the future and the bank said "No. Every time you want to make any changes, he has to ring and authorize you to talk to me again. How ridiculous."

Gillian says,

> All we had to do was tell his name, his date of birth, his mother's maiden name and the account number….If you knew the person you could quite possibly know the mother's maiden name. …To me that is not as secure as being able to send an encrypted email through a banking system. There is no point fighting them. They don't listen.

SCENARIOS: CHANGES IN LIFE STAGES, RESIDENCE, AND RELATIONSHIPS

We draw on our qualitative study to sketch personas and scenarios which illustrate users' problems with money, privacy and the bank.

Scenarios have been successfully used to bridge the different perspectives of users, providers of services and policy makers, while keeping the user at the centre [3]. The stories themselves become a 'boundary object'[19], around which people of different perspectives can come to a shared understanding of user needs. Through the use of personas and scenarios we ensure that we translate insights into user needs to viable strategy and design of technologies. The strategy and design has to be sustainable from three perspectives – the consumers, the providers and the designers. As Norman (1998) said when speaking of the design of technologies, all three legs of the tripod have to work together for success[13].

In the following section we present scenarios that connect with fears over the leakage of personal information; changing relationships and information requirements; and being able to control the way we are represented in the bank through our personal details and financial arrangements.

Ensuring that personal information does not leak out

Barry is an IT professional and knows that the PC was not designed for secure money transactions. He also goes to great lengths to ensure he minimizes the possibility of spam. He would like to use Internet banking because of its immediacy and convenience. He feels he could from his side make his PC and networks sufficiently secure for the low level money transactions he has in mind. But he would like to be assured that the bank will not sell his personal details to telemarketers. At present he does not believe their privacy policies and wonders whether privacy is achievable in a digital world.

User problem: Barry wants proof that the bank's privacy policy is an enforceable contract and that the bank be held accountable if his personal details leak outside the organization.

Design solution: In a reverse form of digital rights management, consumers should be able to track the flow of their personal information. This visual record of how information has not gone outside the organization will help engender trust and boost its brand.

Banking, gender, privacy and joint accounts

Tom and Helen are highly paid professionals in their late 50s. Their children have moved out and their mortgage has been paid. They have a relationship with three banks – their salaries and main payments are with one; savings go into the second and financial investment is done through the third.

Over the years, their mix of individual and joint bank accounts has changed, as has their individual financial status. However their banks continue to see Helen as subsidiary to Tom. Helen continues to note with unease that even when the bank communication is for her, it is addressed to Mr and Mrs… But then information about a personal loan was also sent to her husband. She says,

> I went to borrow money for a holiday house and I was aghast that the bank sent the information to Tom. He had had nothing to do with it. It is not that I did not want him to know, but it was my loan application, not his.

There are some accounts, where Tom is the only account holder. Helen wanted to inform the bank about a change in their address, but they would not accept it from her, as she was not named on that particular account. Helen says, "We would like to tell the bank how it should deal with our financial information, rather than them assuming that all the decisions are made by Tom."

User Problem: The bank is keeping to old stereotypes about money and gender built into banking products and not keeping up-to-date with changes in social norms and within Tom and Helen's family. The bank needs to find a way to honor the individual's preferences for the giving and receiving of financial information.

Design Solution: When Tom and Helen open accounts, the bank asks them to specify how they want their personal information treated through the Privacy Rights Management (PRM) system. This is so that they can influence how they are represented in the bank's information bases. The default choices are the traditional ones. There can be at least two additional choices

allowing Tom and Helen to personalize the way they want to receive and give information. This is also an approach that can be taken to deliver information when it is a community, rather than an individual that owns the money and/or property.

Caring for the mother's finances
James, 45-54 has been caring for his mother's finances since his father died. James' mother used to leave the banking to her husband. At 72, she is wary of the new technologies and the lack of personal contact. In the beginning James would go with his mother so that she could do her weekly banking. She now is used to the local branch. However he would like to pay bills and transfer money on his mother's behalf. His mother would appreciate the help but does not want to sign a third party agreement for it is irrevocable. She trusts James but does not want to cede all control.

User problem: An aged parent would like help with the money management, while at the same time keeping some control over the sharing of information.

Design solution: The parent should be in control of access to information about money and the money in her or his account. However, the parent should also have an easy way of sharing this information so that she can get the help needed.

Stranded when changing country
Jane and her husband moved recently from the United Kingdom to Australia. Before leaving, they informed the bank about their change of address and contact details.

Soon after they arrived in Australia they rented an unfurnished house and bought an unusual number of goods. To their horror they found the bank had cancelled their credit card, after it was unable to contact them at their old address.

Jane tried to call and tell the bank that they indeed were using the card in Australia and here were the new contact details. However the bank insisted that Jane's husband call and make the complaint.

User Problem: Different parts of the bank's information base do not communicate with each other. Hence the bank has different personal data on the customer that remains unconnected.

Design Solution: Users should be able to control the input of a change of details, which then is communicated to all parts of the bank.

Stuck because of direct debit and credit
Ian is a plumber and has been with the bank for 20 years. He is livid because they dishonoured a cheque without trying to contact him. In order to move his account, he has to keep two accounts going for a considerable period to make sure that the direct debit and direct credit instructions have been successfully changed.

User Problem: The convenience of direct debit and credit is negated by users' lack of control over changes or stoppages of direct debit and credit.

Design Solution: Ian should be in control of his direct debit and credit instructions so that he can give the information to his new bank, who then can affect the transfer.

DESIGN OF PRIVACY RIGHTS MANAGEMENT
Privacy Rights Management (PRM) can be used to protect and manage the privacy rights of customers. It has to be a two-tier system. The first level is to ensure that customers' information does not go outside the bank and its designated agents. This level of PRM could give additional comfort to people who at present are not users of Internet banking because of concerns with security and privacy. The second level of PRM ensures that people's privacy references are honored. This will ensure that separate account transactions are not revealed to others without explicit permission. It will also mean people can articulate the way they want their rights on joint accounts to be handled by the bank.

Technologically we see PRM as the mirror image of Digital Rights Management systems (DRMs) that are used to protect and manage the rights of digital copyright owners and manage access to digital information.

The Smart Internet Technology Cooperative Research Centre is exploring whether DRM technology can be used to allow the owner of information, the data subject, to control who has access to his or her personal information and to set the terms by which organizations can access that information. Rather than protecting digital copyright, the technology could be used to shape the sharing of information and thus protect consumers' privacy.

Individuals generally do not object to providing personal information for the purpose of obtaining a service or a product. Their broad concerns relate to whether the information provided is used for the purposes advised by the data acquirer and whether it is disclosed to others inappropriately, without consent. The other more immediate concern is that the customers themselves should be able to set the rules about the sharing of information with partners and family.

Privacy Rights Management (PRM), therefore, gives people the ability to control how far their personal information is disseminated and by whom it is viewed. PRMs can work in a number of ways, such as operating as Trusted Third Parties or as central government agency. What is important is that the controller of the PRM is trusted by individuals. This lack of trust is one reason why government proposals to establish national identity databases meet with suspicion. The approach selected by the SITCRC is for the organization requiring access to personal information, in this case, a bank, to be the provider of the PRM. We see that there will be substantial benefits for the bank in providing the PRM in respect of

identity verification of customers and in differentiating themselves from competitors.

Bank customers will be able to set a few basic rules to be followed by the bank. These rules might cover the way customers want their information shared; and the ways in which they want their information communicated. These could include:

- Rules about a third party's right to information about a customer's accounts

- Rights to change details or report changes on a joint credit card and account; The sending of marketing information to customers

- Preferred ways to contact the customer – email, mobile telephone, fixed line telephone, post.

CONCLUSION

We have conducted a qualitative study of the way 64 people bank and conduct their money relationships. We have focused on how privacy, security, trust and identity influence customers' choices, particularly in regard to Internet banking.

It is important to note that 36 per cent of our sample do not use Internet banking. This is because of low income, security concerns and lack of perceived usefulness. Most of the Internet banking users remain concerned about privacy and security. They either choose to rate convenience over the risks, or try not to think of the dangers.

There is also a feeling that banks are unresponsive and do not help consumers personalize their information and the ways in which they would like to receive and share information.

We translated these consumer insights into personas and scenarios, so that the user can be at the centre of business strategy and the design of services. We think PRM, suitably designed has a role to play in the user-centred design of personalized financial services.

REFERENCES

1. Altman, I. *The Environment and Social Behaviour: Privacy, Personal Space, Territory and Crowding*. Brooks/Cole, Monetery, 1975.
2. Altman, I. Privacy Regulation: Culturally Universal or Culturally-specific? *Journal of Social Issues*, *33* (3). 66-84.
3. Carroll, J.M. Five reasons for scenario-based design. *Interacting with computers*, *13* (1). 43-60.
4. Cowen, Z., Opening Address'. in *Symposium on Privacy*, (Sydney, 1976), University of New South Wales.
5. Federal Privacy Commissioner. Community Attitudes Towards Privacy in Australia, 2000.
6. Glaser, B.G. and Strauss, A.L. *The discovery of grounded theory: Strategies for qualitative research*. Aldine, Chicago, 1967.
7. Hughes, J., O'Brien, J., Randall, D., Rodden, T., Rouncefield, M. and Tolmie, P., Getting to know the 'customer in the machine'. in *Proceedings of the international ACM SIGGROUP conference on Supporting group work*, (Phoenix, Arizona, United States, 1999), ACM Press, 30-39.
8. Kroger, J. *Identity Development: Adolescence Through Adult*. Sage, Tromso, Norway, 2000.
9. Lambert, L. Asian Underground Banking Scheme: A Field Note. *Journal Of Contemporary Criminal Justice*, *18* (4). 358-369.
10. Miller, D. and Slater, D. *The Internet: An ethnographic approach*. Berg, Oxford, 2000.
11. Morison, W. Report on the Law of Privacy *New South Wales Parliament,*, 1973, para 4.
12. Morse, J.M. and Richards, L. *Readme First for a User's Guide to Qualitative Methods*. Sage Publications, Thousand Oaks, Calif., 2002.
13. Norman, D.A. *The Invisible Computer*. MIT Press, Cambridge, Mass, 1998.
14. Princeton Survey Research Associates International. Leap of Faith: Using the Internet despite the Dangers- Results of a National Survey of Internet Users for Consumer Reports WebWatch, Consumer Reports WebWatch, New York, 2005.
15. Saunders, K.M. and Zucker, B. Counteracting identity fraud in the information age: The Identity Theft and Assumption Deterrence Act. *International Review of Law, Computers & Technology*, *13* (2). 183.
16. Singh, S. Impersonalisation of electronic money: Implications for bank marketing. *The International Journal of Bank Marketing*, *22* (7). 505-521.
17. Singh, S. and Cassar-Bartolo, K., The privacy of money and health. in *OZCHI*, (Wollongong, 2004).
18. Singh, S., Zic, J., Satchell, C., Bartolo, K.C., Snare, J. and Fabre, J., A Reflection on Translation Issues in User-Centred Design. in *7th International Conference on Work with Computing Systems, WWCS 2004*, (Kuala Lumpur, 2004).
19. Star, L.S. and Griesemer, J.R. Institutional Ecology, 'Translations' and Boundary Objects. *Social Studies of Science*, *19* (3). 387-420.
20. Turkle, S. *Life on the Screen: Identity in the Age of the Internet*. Simon and Schuster., New York, 1995.
21. Vinge, V. Introduction. in Frenkel, J. ed. *True Names and the opening of the cyberspace frontier*, Tom Doherty Associates, New York, 2001, 15-23.

22.   Vredenburg, K., Isensee, S. and Righi, C. *User-Centered Design: An Integrated Approach*. Prentice Hall, Upper Saddle River, NJ, 2002.
23.   Warren, S. and Brandeis, L. The Right of Privacy. *Harvard Law Review*, *4* (193).
24.   Westin, A. *Privacy and Freedom*. Atheneum, New York, 1967.