# ANZAM PAPER 2006

## Australian banks' approaches to privacy in an online world:

## How well do their policies measure up to the national principles?

Greg Cranitch
*School of Information and Communication Technology, Griffith University, Queensland, Australia.*
Email: g.cranitch@griffith.edu.au

Prof. Tom Nguyen
*Department of Accounting, Finance and Economics, Griffith University, Queensland, Australia.*
Email: t.nguyen@griffith.edu.au

Dr Anne Nguyen
*School of Information and Communication Technology, Griffith University, Queensland, Australia.*
Email: a.nguyen@griffith.edu.au

# Australian banks' approaches to privacy in an online world:

# How well do their policies measure up to the national principles?

**ABSTRACT**

Around the world, there have been many examples of individuals whose personal and financial information was disclosed to unauthorised individuals. In Australia, privacy legislation has been enacted with a view to preventing such abuses. In particular, the national privacy principles detail how private-sector organisations should handle and protect their clients' personal information. How well do financial institutions measure up to those principles? In this study, the privacy policies of 18 Australian banks are assessed against the national principles. In general, the results are fairly reassuring. Nevertheless, some areas of concern remain, particularly where trans-border outsourcing of some information processing tasks is involved.

***Keywords****: Privacy policies; national privacy principles; Australian banks; Internet banking; online banking; offshore outsourcing.*

## 1. BACKGROUND: INTERNET BANKING AND PRIVACY ISSUES

During recent years, e-commerce has grown at phenomenal rates. Moores (2005) reported that e-commerce sales in the US experienced significant growth even at a time when the economy was close to a recession. Yet he also sounded a cautionary note, warning that concerns over privacy issues would probably lead to substantial lost online sales in the future.

These general observations hold particularly well with respect to the banking and finance sector. According to a survey conducted in late-2004 by the Pew Internet and American Life Project (PIP), the number of users of online banking in the US had reached 53 million (about one-quarter of the adult population, and 44% of American internet users), an increase of 47% over two years (Fox, 2005). Indeed, of all the major internet activities monitored by the PIP, online banking has grown the fastest.

In Australia, banks have encouraged customers to do more of their banking business online. In recent years, many bank branches have been closed, and changes in fee structures have made branch transactions more costly relative to the use of automatic teller machines (ATMs) and telephone and internet banking. A survey conducted for the major Australian banks estimated that the number of online bank accounts grew by 25% each year since December 2003 (Lion, 2005).

This rapid growth in online banking may be slowing, however, in both the US and Australia, due partly to privacy and security concerns. In another US survey, completed by Ipsos Insight, it was found that the percentage of respondents who conducted some banking online in August 2005 was the same as that recorded 12 months earlier, indicating a flattening trajectory after "years of dramatic growth in online banking penetration" (Cottings, 2005). A very large majority (73%) of the Ipsos sample indicated that they regarded the possible theft of their personal information (mainly a security issue) as a significant deterrent. In the same vein, 72% were very concerned that the banks might make their personal information available to others for a fee (a privacy issue). This paper focuses mainly on privacy issues, while keeping in mind that, of course, security and privacy are closely inter-related in practice.

There is a sizable and growing range of technical solutions to data security as a general concern. For example, banks often highlight their use of encryption as a means of protecting data sent over their networks. Encryption will certainly reduce the risk of data being intercepted clandestinely. However, it provides no safeguard against the possibility that the information may be misused or improperly disclosed once it has been collected and stored. Accordingly, privacy policies are required to address this and related issues.

Privacy is an important aspect of the relationship between an individual and society. In essence, it is the right of individuals to limit and control how much society knows about them and their interactions with other persons or organisations. Conceptually, privacy can be thought of in terms of three dimensions: anonymity, confidentiality, and security (Rainie, 2004). Anonymity means that, e.g., online consumers can complete their transactions without being identified or known. Confidentiality means that while it is appropriate for an organisation to disclose the information that it has collected about an individual to someone else in order to complete the relevant transaction, it is unacceptable for the organisation to disclose it to others for unrelated purposes and without the individual's permission. Security requires that those who receive the information protect it from theft or unauthorised use.

In the Universal Declaration of Human Rights, adopted by the United Nations in 1948, privacy is recognised as a fundamental human right. Different countries, however, adopt different approaches to privacy protection. It is generally acknowledged that the EU has a stronger privacy legislative framework than the US, and that Australia falls somewhere between them; see, e.g., Scribbins (2001) and Markey (2005). According to a league table compiled for the Markey report, of the 20 countries and regions surveyed, Canada, the EU and Hungary receive the top rating (denoted "A"); while Australia, the Czech Republic, Japan, and Hong Kong receive the next highest rating (a "B"); compared with a "C" for the US and Korea; and a "D" for countries like India and Singapore.

In principle, the overall notion of privacy encompasses bodily integrity, and protection of home and possessions, including private communications. In the current context, the protection of privacy requires *the establishment and implementation of rules that govern and limit the collection, processing, and use of personal information that is revealed by individuals during their interactions with companies and other organisations.* This is also often referred to as “data protection” (Scribbins, 2001).

Computers and the Internet allow companies to collect, at relatively low costs, a much larger volume of personal information as a by-product of online transactions than was feasible previously. With so much personal data being collected and stored electronically, the risk of some of the information being misused or disclosed without the express consent of the individuals concerned has also increased considerably.

In June 2005, there was widespread media coverage of CardSystems, a US credit card processing company, which had inadvertently allowed the details of 40 million customers to be compromised; see, e.g., Riley (2005). Nor was this an isolated incidence; see, e.g., the cases of ChoicePoint (*Money*, 2005) and Citigroup (Reuters, 2005). Indeed, in mid-2005 it would appear that there was "a wave of security breaches and lapses that calls into questions the security of electronic and financial transactions" (Camp et al, 2006: 6.1).

## 2. RESEARCH QUESTIONS

Because of concerns over security and privacy breaches, most people will only do business online with individuals and institutions that they trust. If a company or organisation has a privacy policy that clearly and credibly specify how issues relating to anonymity, confidentiality and security are managed, this will tend to increase the probability that consumers will trust the company. In a study conducted by Consumer International in 2000, it was found that 58% of the web sites (mainly in the US and EU) that collected personal information about their visitors had a privacy policy (Scribbins, 2001). However, this proportion varied across the types of web sites studied: *health-related* sites were least likely to have such a policy, while US-based *banking and finance* sites were far more likely to have them. Among the *most popular* US sites studied (these include portal sites, email and internet service providers, news and weather sites, and the like) the ratio reached 100%.

A more recent study by Ryan (2005) found that, of 127 e-business web sites examined, only 27.6% had a privacy policy posted on their own site. How do Australian bank web sites compare with these two international samples? The current study will address, among other things, this question.

In order to conduct their business, banks often need to have information about their customers' income, employment status, financial commitments, current and previous loans, and so on. In some cases, they may also need to record other sensitive personal information, such as details regarding previous illnesses, to support related activities (e.g. insurance). It is essential that all such collected information be protected against misuse and unauthorised disclosure.

The Australian Government has enacted legislation to protect personal information. The first such legislation was the Privacy Act 1988 (Cwth). In 1991 the Credit Reporting Code of Conduct was issued as a complementary code to the Act, and serves as binding law on credit providers and credit reporting agencies. The Privacy Amendment (Private Sector) Act 2000 amended the Privacy Act 1988 to include provisions that regulate the way private-sector organisations deal with personal information. A key feature of the new legislation was a list of 10 national privacy principles (NPPs), governing how organisations should collect, store, use, disclose, and keep secure personal

information. They also require that the individual in question be allowed access to his or her own personal information (see Table 1).

In view of recent international studies and the legislated national principles, this paper seeks to assess:

(1) whether Australian banks display their privacy policies on their web sites; and

(2) whether these policies meet the 10 National Privacy Principles.

The answers to these questions are likely to be of interest to many Australians as well as international observers of online banking, electronic finance, and privacy protection generally. The next section of the paper provides details of the methodology used to obtain these answers.

**Table 1. National Privacy Principles**

| |
|---|
| **NPP1: Collection** — describes the ways in which an organisation can appropriately collect customers' personal information. |
| **NPP2: Use and Disclosure** — outlines how organisations can properly use and disclose personal information. |
| **NPP3: Data Quality & NPP4: Data Security** — set the standards that organisations must meet for the accuracy, currency, completeness and security of personal information. |
| **NPP5: Openness** — requires organisations to be open about how they handle personal information. |
| **NPP6: Access & Correction** — gives customers a general right of access to their own personal information, and the right to have that information corrected, if it is inaccurate, incomplete or out of date. |
| **NPP7: Identifiers** — says that, in general, Commonwealth government identifiers (such as the Medicare number or the Veterans Affairs number) can only be used for the purposes for which they were issued. |
| **NPP8: Anonymity** — where possible, requires each organisation to provide the opportunity for customers to interact with it without identifying themselves. |
| **NPP9: Trans-border Data Flows** — outlines privacy protections that apply to the transfer of personal information out of Australia. |
| **NPP10: Sensitive Information** — requires the customer's consent when an organisation collects sensitive information about the customer, such as health information, or information about racial or ethnic background, or criminal record. Sensitive information is a subset of personal information and special protection applies to this information. |

Source: http://www.privacy.gov.au/privacy_rights/ypao/index_print.html#summary

## 3. METHODOLOGY

The Australian Government's privacy principles, as listed in Table 1, were used as a basis for developing a survey instrument. Specifically, a template of the 10 NPPs was developed, and converted into a questionnaire. The latter also covered three additional issues/questions, as detailed below. The web sites of selected Australian banks were assessed by a single reviewer using this questionnaire. The banks included in the survey are listed in Table 2. These are the largest banks in Australia, each accounting for around 1% or more of the total resident asset value of all Australian commercial banks. (Each of the 4 biggest banks accounted for around 15%-20% of this total.) The combined asset value of the 18 banks surveyed amounted to 94.8% of the total for all banks.

**Table 2. Australian Bank Web Sites Considered**

| Banks | % Total Assets * | Access |
|---|---|---|
| ABN AMRO Bank | 1.0 | http://www.abnamro.com.au, accessed 4 May 2006 |
| Adelaide Bank | 0.9 | http://www.adelaidebank.com.au, accessed 25 Aug 2005. |
| Australia & New Zealand Bank | 14.7 | http://www.anz.com.au, accessed 25 Aug 2005. |
| Bank of Queensland | 0.9 | http://www.boq.com.au, accessed 25 Aug 2005. |
| Bank of Western Australia (& HBOS Treasury Services) | 3.7 | http://www.bankwest.com.au, accessed 25 Aug 2005. |
| Bendigo Bank | 1.0 | http://www.bendigobank.com.au, accessed 25 Aug 2005. |
| Citibank (& Citigroup) | 1.7 | http://www.citibank.com.au, accessed 25 Aug 2005. |
| Commonwealth Bank of Australia | 19.2 | http://www.commbank.com.au, accessed 25 Aug 2005. |
| Deutsche Bank | 1.4 | http://www.deutschebank.com.au, accessed 4 May 2006 |
| HSBC | 1.3 | http://www.hsbc.com.au, accessed 4 May 2006 |
| ING Bank (Australia) | 2.2 | http://www.ing.com.au, accessed 25 Aug 2005. |
| Macquarie Bank | 2.3 | http://www.macquarie.com.au, accessed 4 May 2006 |
| National Australia Bank | 18.1 | http://www.national.com.au, accessed 25 Aug 2005. |
| Rabobank (& Co-Operative Central Raiffeisen-Boernenleenbank ) | 1.2 | http://www.rabobank.com, accessed 4 May 2006 |
| Societe Generale | 1.3 | http://www.au.sgib.com.index.htm, accessed 4 May 2006 |
| St George Bank | 5.8 | http://www.stgeorge.com.au, accessed 25 Aug 2005. |
| Suncorp Metway | 2.9 | http://www.suncorp.com, accessed 25 Aug 2005. |
| Westpac Banking Corporation | 15.3 | http://www.westpac.com.au, accessed 25 Aug 2005. |
| **Total** | 94.8 | |

*** Source**: Data on shares of the total resident asset value of the banking sector are obtained from Australian Prudential Regulation Authority (2006).

The web site for each bank was carefully perused to determine whether a privacy policy was displayed onsite (Question 1). The assessment also took into account the location and mode of the

display itself on the web site (Question 2), and whether the policy statement addressed each of the 10 NPPs (Questions 3 to 12). A related question was whether each web site provided information and warnings to customers regarding its use of internet "cookies" (Question 13).

## 4. RESULTS AND DISCUSSION

Table 3 presents a summary of the assessment of each web site with respect to the 13 questions contained in the questionnaire. For confidentiality, the banks' names have been replaced with identifying numbers which were allocated randomly, apart from the fact that Banks B1 to B4 represent (in no particular order) the four biggest banks (all locally owned), and Banks B15 to B18 represent the four foreign banks with branches in Australia and with sufficient resident assets to be included in the survey. Banks that are subsidiaries of foreign banks are listed in between these two groups, as are smaller locally owned banks. In each cell, "y" indicates "yes"; for "no", the cell would be left blank to facilitate recognition of the overall pattern.

All of the surveyed banks addressed the first NPP, as shown along Row 3 of the table. All banks noted that they collected personal information that was necessary for them to complete transactions with their online customers. It was also clear that if information was not provided then the transaction could not be completed. NPP 2 was also addressed explicitly by all banks (see Row 4). Each bank stated its policy on the use and disclosure of any information collected, including the type of individuals and organisations to whom it may disclose the information. Similarly, all banks made it very clear that they regarded data quality and data security (NPPs 3 and 4) as very important. But the statements were made in general terms, and typically there was no elaboration as to how the bank would ensure quality or security. It would appear that banks expected customers to trust their word that they would do what they stated.

As discussed above, all the banks made available via their web site a copy of their privacy policy. They also made known the type of information they collected. Thus NPP 5, in relation to openness, was addressed by all banks. Further, all the web sites displayed relevant contact details and

procedures that would allow individuals to apply for access to the stored information as it relates to themselves, and to correct the information if necessary, thus satisfying NPP 6.

The above results demonstrate a remarkable degree of similarity among the examined bank web sites with respect to their approaches to the first six NPPs, as shown by the solid block of "y" along the relevant rows and columns of Table 3. By contrast, principles 7 to 10 are where differences started to appear in the banks' privacy statements.

Organisations generally find it useful to have a means to uniquely and quickly identify the records associated with an individual member or customer. This is usually a unique number, as other personal information will typically not guarantee a unique key. Australia does not have a national identity card system, but a number of commonwealth (national) government identifiers already exist and can be used to quickly identify an individual, although none of these is universal, in that none has been issued to *all* Australians. Examples of commonwealth identifiers include the tax file number, Medicare number, Centrelink (social security) number and Veteran Affairs number.

NPP 7 regulates how commonwealth government identifiers may be used. These identifiers can only be used as the primary means of identification for the purposes for which they were issued (e.g., taxation, medical care, and so on). Banking was not one of these.[1] Even so, only 39% of the sites stated explicitly that they did not use these identifiers as the primary means of identifying an individual. The others made no mention at all as to whether and how they used these identifiers. In practice, however, the banks are under constant government scrutiny to ensure that they comply with the various prudential requirements and financial regulations. In addition, the possible use of various commonwealth government identifiers as a quasi-national identity scheme has long been a prominent, and controversial, issue. Together, these mean that bank customers would be reasonably safe in assuming that their bank, even if it were one of those that made no mention of this issue on their web site, would not be using the identifiers illegally.

[1] Nevertheless, a document containing both personal details and the relevant identifying number may be used by a potential bank customer as a supplementary form of identification to help confirm his/her identity.

**Table 3. Summary of Survey Results**

| | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 | B12 | B13 | B14 | B15 | B16 | B17 | B18 | #y | %y |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Link to privacy policy displayed | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | 18 | 100 % |
| Link prominent on home page | y | | | y | y | y | | y | y | y | y | y | | | | y | y | | 11 | 61% |
| NPP1: Collection | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | 18 | 100 % |
| NPP2: Use and Disclosure | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | 18 | 100 % |
| NPP3: Data Quality | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | 18 | 100 % |
| NPP4: Data Security | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | 18 | 100 % |
| NPP5: Openness | y | y | y | y | y | y | y | y | y | y | Y | y | y | y | y | y | y | y | 18 | 100 % |
| NPP6: Access & Correction | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | y | 18 | 100 % |
| NPP7: Identifiers | y | y | | y | | | | | | y | y | y | | | y | | | | 7 | 39% |
| NPP8: Anonymity | y | | | y | | | | | | y | y | y | | | | | | | 5 | 28% |
| NPP9: Transborder Data Flows | y | | y | | | y | | | | | y | y | | y | y | y | y | | 9 | 50% |
| NPP10: Sensitive Information | y | y | | y | y | y | | | | y | y | | y | | | | y | y | 10 | 56% |
| Warnings about Internet Cookies | | y | y | y | y | y | y | y | y | y | y | y | y | Y | y | | y | y | 16 | 89% |

Only a small minority (28%) of the bank web sites specifically addressed NPP 8, which relates to anonymity. Upon reflection, this is not too surprising, as most dealings between a customer and a bank are in relation to existing accounts, loan applications, insurance policies or claims, and the like. In such cases, an individual's identity must be known and verified to complete the transaction. There is very little that can be done with a bank anonymously, other than enquiries of a very general nature.

Only 50% of the bank web sites addressed NPP 9, which governs the trans-border flow of personal data. In principle, therefore, customers of half of the banks (including two of the four largest banks) would have no idea whether their bank sends their personal information overseas or not, and if it does, how it intends to manage the related privacy issues.

Moreover, none of the banks stated categorically that their back-office processing was completed wholly within Australia; while only one bank (a branch of a foreign bank) explicitly stated that some of its processing and data storage was performed offshore at one of its other branches. No other bank made explicit statements, one way or the other, about this issue of offshore processing. Yet these are highly relevant questions, as there is a growing trend for Australian businesses to outsource back-office processing and call-centre operations overseas. How a bank ensures that the offshore centre will adhere to the bank's stated privacy policy was usually not addressed in the policy statement itself.

Only 56% of the banks specified how they deal with sensitive information (NPP 10). However, this is probably not as much a source of concern as it may appear at first, because not all of the banks have insurance companies associated with them, and consequently many banks do not need to collect health and other sensitive information at all. An overwhelming majority (89%) of the surveyed web sites acknowledged that they used cookies and described how they used them. Often the bank in question required the use of cookies so that it would know where the customer has got up to in a multiple-page transaction.

The results presented in Table 3 do not display any obvious differences in approaches to privacy between the four biggest banks as a group (often called the "majors" in Australia) and the remaining banks. Nor are there any obvious "outliers". Only one bank (B11) receives a "y" rating for every

question considered, but it is not really an outlier as there are several others with only one "y" missing. At the other end, no bank stands out clearly as displaying too few "y" ratings compared with the others. Interestingly, three (i.e., 75%) of the four foreign bank branches receive a "y" rating on NPP 9 (trans-border data flows) compared with 50% of the entire sample. However, the sample sizes are too small to conclude whether this difference is significant.

From the viewpoint of the bank customers, it is encouraging that all 18 sites were rated "y" on the first question (was the privacy policy accessible?) and on NPPs 1 to 6. Moreover, on each of the remaining 6 questions (prominence of the display of the privacy policy; national principles 7 to 10; and warning regarding cookies) the "y" rating was generally given to at least 39% of the sites. The only exception was NPP 8, regarding anonymity, on which only 28% of the sites received the "y" rating, but which, as discussed above, is often not a highly relevant issue in the context of banking transactions. Overall, this would appear to be a set of fairly reassuring results for customers of Australian banks. Nevertheless, a number of concerns do remain.

## 5. REMAINING CONCERNS

A major concern relates to trans-border data flows (NPP 9), especially those involved in back-office processing operations that have been outsourced overseas. In their posted statements, the banks often stated that their staff must adhere to strict policies and procedures, and that their business partners are to use personal information only for the purpose for which they have been given access to the data. Typically no statement was provided regarding how adherence to the stated policies by bank staff and business partners would be ensured.

Implicitly it would be reasonable for customers to assume that each bank would be responsible for the professional conduct of its own employees. By contrast, it is uncertain as to how well a bank might police the operations of its business partners, and how readily it would accept responsibility for the operations of such partners. In the past, in auditing credit providers for compliance with the Privacy Act, the Australian Privacy Commissioner has found that the outsourcing contracts that these credit providers signed with other firms, especially record management agents, often failed to include

clauses which would help to protect personal and financial information against loss and unauthorised access (Privacy Commissioner, 1996).

McCabe (2005) presented two instructive examples, involving Telstra Bigpond Music and Amazon.com, both of which outsourced the order-filling process. In each case, the external service provider was not able to complete the online transaction satisfactorily, and the customer was asked to resolve the matter with this contracted third party. In situations like these, it is understandable that customers would become disenchanted. Although the outsource service provider is responsible to the procuring (client) company for processing the order, it is the latter company with whom the customer placed the order originally, not the former. Ideally, therefore, if a bank outsources an activity and errors are made, then the bank should be responsible for fixing them, and in the process should liaise with the external company as required. The bank customers should not have to deal on any extended basis with the third-party company. None of the web sites surveyed made clear that this would be the case.

The above concerns (over the conduct of third-party companies and the division of responsibility between such contracted third parties and the original bank) become even more serious in the cases where the contracted company is located overseas. In dealing with Australian companies, customers could rely on the knowledge that personal information provided to such companies would be covered by Australian legislation. If, however, the company is outside Australia and is not subject to Australian or equivalent legislation, the customers may receive very little legal protection:

> "Generally, once information goes beyond Australia's borders, it will be either impractical or impossible for a client [contracting company] to prevent unauthorised use or disclosure." (Privacy Commissioner, 1996: Clause 6).

This assessment appears to be borne out by number of recent cases around the world. In October 2003, the University of California at San Francisco Medical Center received threats from a disgruntled outsourcing worker in Pakistan to post confidential patient records on the Internet unless the hospital helped to redress her grievances over unpaid wages (Lazarus, 2004). See also the case of MphasiS (Carretek, 2005) and the reports that Indian call-centre employees had sold personal details of British and Australian customers (Associated Press, 2005; Offshore Outsourcing Best Practices, 2005).

Ahmed (2005) pointed out that in India, where business process outsourcing (BPO) has grown particularly fast during the past 5 or so years, staff turnover is high, and the management of IT security is often "not up to the mark". It is estimated that about 80% of BPO companies there do not use integrated security management tools, and about 10-25% of applicants for call centre jobs provide false or incorrect information about themselves. Moreover, many employers fail to perform adequate background security checks on workers performing the outsourced operations. From these, it would seem reasonable for Australian bank customers to be concerned about the security and confidentiality of their personal information if the processing of such information is outsourced overseas. Do the contracted partners have the capacity to process data securely? This remains an important question.

What are the responsibilities of Australian banks with respect to privacy protection in this context? Under NPP 9, they should ensure that, among other things:

(a) the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the NPPs; and

(b) the information which is to be transferred will not be held, used or disclosed by the recipient in a manner inconsistent with the NPPs.

(National Privacy Principles, extracted from the Privacy Amendment (Private Sector) Act 2000)

The key question, then, is how Australian banks can ensure these conditions are met. Condition (a) is about the equivalence to Australian standards of legal means to protect privacy in the overseas country. EU companies wishing to do business with US companies faced a similar problem in the late-1990s, as they were required to ensure that their overseas business partners offer the same degree of protection adequacy as afforded by EU regulations, and yet US privacy regulations were generally considered less stringent than those of the EU [2] .

[2] One of the key differences is that the US adopts a sectoral approach to data protection, enacting legislation governing telecommunications, banking and finance, health, etc. separately, rather than an overall framework as in the EU.

After lengthy negotiations, in July 2000 the EU agreed to a set of "Safe Harbour" arrangements designed to allow US companies to opt in and to be considered "adequate" by EU standards in these respects. Critics have described this decision as a weakening of privacy protection for EU consumers (Scribbins, 2001). Similarly, given that Australia's privacy protection framework is among the world's stronger regimes, offshore outsourcing is likely to present challenges to ensure that this "equivalence" or "adequacy" condition is met, as most of the countries that are regarded as attractive destinations for the outsourcing tend to have far less stringent legislation. [3]

As for condition (b), which relates to actual compliance, it should be noted that a strong regulatory regime is neither necessary nor sufficient for this to be assured. In principle, even where the national regime is relatively weak, a company with an excellent reputation may voluntarily exceed the national standards to safeguard its brand name and business position. Conversely, even in countries with the most stringent regulations, there will inevitably be some who break the law. Nevertheless, most people would expect that there is some correlation between the two in practice. Further, it is generally more feasible to monitor compliance and, if breaches occur, to seek legal redress domestically than in a foreign country.

Karat et al (2006) found that the privacy policies posted by e-businesses in general were often very vague. The published policies examined in this study also tended to be vague and non-specific. The banks might justify this on the grounds that they do not want to let outsiders know how they implement their policies, as the less known about their implementation, the less chance of outsiders breaching the policy.

Another possible explanation is that while banks are willing to follow national guidelines and principles regarding privacy protection, they are not particularly enthusiastic about providing more information, or greater commitment, in this area than is necessary – with the level of necessity being dictated both by government guidelines, and by what their competitors are doing. Seen in this light, the fact that most banks appear to be in lockstep with one another with respect to privacy policies

[3] In dealing with EU companies, it is Australian companies that would be in the position of having a weaker privacy protection regime, and would have to find ways to prove "EU-adequacy" (i.e., equivalence to EU standards).

suggests that if greater and more genuine competition among banks could be engendered in this area (e.g., through greater customer awareness and demands) banks' privacy policies would probably be enhanced in terms of clearer and more specific commitments, including those relating to enforceability.

## 6. SUMMARY AND IMPLICATIONS

All of the 18 bank web sites surveyed in this study displayed links to their privacy policy on the home page. Further, all of them addressed the first six national privacy principles. Most also acknowledged that they used cookies. Overall, the results are fairly reassuring for Australian bank customers. Nevertheless, some areas of concern remain. In particular, where trans-border outsourcing of some information processing tasks is involved, it is not clear whether and how Australian privacy principles are adhered to in countries where privacy legislation is less stringent than in Australia.

How should the *consumers* respond to all this? In a nutshell, they should be more vigilant. Consumers who have had Internet-related problems with banking losses are often affected very badly indeed. But many consumers may not even be aware that their personal information has been compromised, and many dissatisfied consumers never complain. As Hyman et al (1992: 97) put it, "only a portion of the problems/defects that exist are actually perceived; only a portion of those perceived are voiced; only a portion of those voiced gain access to a complaint-resolving party; and only a portion at each stage are resolved successfully".

It would seem that consumers often will not take the trouble to do simple tasks like reading brochures, learning about their privacy rights and their bank's privacy policies, finding out about possible fraud and other risks and how to avoid them, or checking their bank statements. In the final analysis, consumers must assume responsibility for their own protection (Sullivan, 2006). While the benefits of internet banking (including greater convenience) are considerable, there are also many security risks, and this is one instance where caution and efforts to keep abreast of developments are likely to pay off well in terms of better management of such risks.

## REFERENCES


Ahmed, Z. (2005), Outsourcing exposes firms to fraud, BBC News International Edition, 16 June 2005, http://news.bbc.co.uk/2/hi/business/4094894.stm, accessed 29 Aug 2005

Associated Press (2005), India to tighten laws to prevent ID theft, 30 June 30, http://www.msnbc.msn.com/id/8404104/, accessed 29 April 2006.

Australian Prudential Regulation Authority (2006), *Monthly Banking Statistics for February 2006*, issued 31 March.

Camp, J., S. Goodman, C. House, W. Jack, R. Ramer, and M. Stella (2006), Chapter 6: Offshoring: Risks and exposures, in *Globalization and Offshoring of Software*, edited by W. Aspray, F. Mayadas, and M. Vardi, Association for Computing Machinery, Job Migration Task Force, February.

Carretek (2005), The MphasiS scandal – And how it concerns U.S. companies considering offshore BPO, June, http://www.carretek.com/main/news/articles/MphasiS_scandal.htm, accessed 23 April 2006.

Cottings, D. (2005), Interest in online banking flattens, Ipsos Insight, http://www.ipsos-insight.com/pressrelease.aspx?id=2765, accessed 18 Oct 2005.

Fox, S. (2000), Trust and privacy online: why Americans want to rewrite the rules, Pew Internet and American Life Project, Report, 20 August.

Fox, S. (2005), The state of online banking, Pew Internet and American Life Project, Data Memo, February.

Hyman, D., J. Shingler, and M. Miller (1992), Consumer complaints and the public policy: validating the "tip-of-the-iceberg" theory, *Sociological Practice*, Vol. 10.

Karat, M., C. Brodie, and J. Karat (2006). Usable privacy and security for personal information management, *Communications of the ACM*, Vol. 49, No. 1, pp. 56-57.

Lazarus, D. (2004), Outsourced UCSF notes highlight privacy risk, San Francisco *Chronicle*, 28 March.

Lion, P. (2005) Banking on Net fast becoming the norm, *The Courier Mail*, 11 October, p. 21.

Markey, E. (2005), Outsourcing privacy: Countries processing US social security numbers, health information, tax records lack fundamental privacy safeguards, Staff Report, US House of Representatives, September.

McCabe B. (2005) Trust must be earned online, *The Australian*, 5 July, p 2.

*Money* (2005), ChoicePoint: More ID theft warnings, 17 February, http://money.cnn.com/2005/02/17/technology/personaltech/choicepoint/index.htm, accessed 28 April 2006.

Moores T. (2005) Do Consumers Understand the Role of Privacy Seals in E-Commerce?, *Communications of the ACM*, Vol. 48, No. 3, pp. 86-91.

Offshore Outsourcing Best Practices (2005), Indian BPO providers tighten data security, 20 November, http://www.oobp.org/Outsourcing+News/444.aspx, accessed 23 April 2006.

Office of the Australian Privacy Commissioner (2005), *Getting in on the Act: The review of the private sector provisions of the Privacy Act 1988*, Review Report, March.

Privacy Commissioner (1996), *The handling of credit reports by records management agents and other contractors: Advice for credit providers and credit reporting agencies when contracting out record management functions*, May.

Rainie, L. (2004), Trust and Privacy online: What the public really wants, Franklin & Marshall College Privacy Class notes, http://www.pewinternet.org/ppt/Lee Rainie, accessed 21 April 2006

Reuters (2005), Citigroup data on 3.9 million goes missing, 6 June, published on *ZDNet News*, http://news.zdnet.com/2100-1009_22-5733971.html, accessed 28 April 2006.

Riley, J. (2005), Call to tighten security on cards, *The Australian*, 5 July, p. 2.

Ryan, J. (2005) Protecting Private Information on the Internet: A Study of Web Server Security and Privacy Policies, *Proceedings of 5th Hawaii International Conference on Business*, Hawaii, USA, May, 2639 – 2647.

Scribbins, K. (2001), Privacy@net: An international comparative study of consumer privacy on the internet, Consumers International, http://www.consumersinternational.org., accessed 23 April 2006.

Sullivan, B. (2004a), ID theft victims face tough bank fights, MSNBC Online Banking Special Report, 18 February, http://www.msnbc.msn.com/id/4264051/, accessed 28 April 2006.

Sullivan, B. (2004b), Survey: 2 million bank accounts robbed, MSNBC Online Banking Special Report, 14 June, http://www.msnbc.msn.com/id/5184077/, accessed 28 April 2006.

Sullivan, B. (2006), Few takers for free credit monitoring, MSNBC The Red Tape Chronicles, 20 April, http://redtape.msnbc.com/2006/04/few_takers_for_.html, accessed 28 April 2006.