Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2007 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

2007

Evaluating Banking Websites Privacy Statements – A New Zealand Perspective on Ensuring Business Confidence

A S C Hooper
Victoria University of Wellington, Tony.Hooper@vuw.ac.nz

B Bunker
Victoria University of Wellington

A Rapson
Victoria University of Wellington

A Reynolds
Victoria University of Wellington

M Vos
Victoria University of Wellington

51. Evaluating Banking Websites Privacy Statements – A New Zealand Perspective on Ensuring Business Confidence

Hooper, A S C Bunker, B Rapson, A Reynolds, A Vos, M
School of Information Management
Victoria University of Wellington
Tony.Hooper@vuw.ac.nz

Abstract

Because banks deal with highly personal detailed and sensitive information, they need to establish and maintain the confidence of their customers more assiduously than most other businesses. The rise of internet banking and the advantages to be gained from the garnering of personal data from websites places banks in a position to exploit customer data in a way that might infringe ethical considerations. This investigation analyses the website privacy statements of New Zealand banks in terms of the provisions of the New Zealand Privacy Act. The intention was to find an objective basis for the assessment of business integrity, to explore how confidence in electronic commerce can be assured. The investigation finds that the use of privacy legislation principles as a means of evaluating website privacy statements is revealing and convincing. It is considered that customer confidence will increasingly impact on Internet businesses, and business integrity as demonstrated by comprehensive and relevant privacy statements will go a long way to provide those assurances.

Keywords: Banking websites, customer confidence, privacy statements, business integrity

Introduction

It is a reasonable assumption that Internet websites are intended to reflect the values of the institutions that sponsor them. Banks, more than other businesses, deal with highly personal, detailed and sensitive information about their customers' purchasing patterns, size of wallet, brand and vendor choices, and other data critical to market intelligence. Banks also make heavy use of the technological advantages of electronic commerce, giving them an opportunity to gather, analyze and possibly sell customer data to affiliated businesses. One could argue, therefore, that banks should be particularly diligent about ensuring that their websites reflect the values they wish to convey to their clients.

While usually happy to exploit the advantages of internet banking, customers are often not aware of the personal information that their banks gather about them and their commercial activities. By publishing a privacy statement on their website, indicating how customer information will be gathered and managed, banks can establish and maintain the confidence of their customers, assuring them of their concern for protecting the integrity of the personal information they handle.

Accordingly, one could argue that the primary criteria for evaluating website privacy statements would be the provisions of the privacy legislation relevant to the country concerned. Most countries operate under different privacy legislation, although there are internationally agreed principles on which most countries legislation is based. The New Zealand Privacy Act of 1993 is technology neutral and based on principles developed in 1981 by the Organization for Economic Cooperation and Development (OECD, 1981). Because of the commonality of the principles of the New Zealand Privacy Act, it was considered that investigating privacy statements on the websites of seven New Zealand banks would give preliminary insights into the integrity of Internet banking. The intention was to explore

whether privacy principles might be applied as a basis for assessing banking websites for responsible business practice in electronic commerce.

This preliminary investigation was carried out as a class assignment by graduate students in the Master of Information Management programme of the Victoria University of Wellington. Data gathered by four students were analyzed and combined in order to identify common findings. While the original intention was to find an objective basis for the assessment of business integrity, it is expected that a basis for promoting customer confidence might emerge.

Literature review

While most consumer commercial transactions require the exchange of some level of personal information, inherent in any understanding of privacy within the context of e-commerce is the individual's right to know (and control) what personal information is being captured and with whom its shared (Mason et al., 2001). In 1981, the Organisation for Economic Cooperation and Development (OECD) considered the issue of privacy with respect to information gathered about individuals and set down eight principles of privacy protection (OECD, 1981). These principles formed the policy basis for the New Zealand Privacy Act of 1993. That Act addresses the handling of all personal information collected or held by agencies, whether in the public or private sectors. Personal information is defined by the Privacy Act (1993) as information about an identifiable individual including information relating to a death as maintained by the Registrar-General pursuant to the Births, Deaths, and Marriages Registration Act 1995, or any former act. Section 6 of the New Zealand Privacy Act sets out twelve information privacy principles that define how both public and private sector agencies must manage collection, use, retention, disposal and sharing of personal information (NZ Privacy Commission, 1994). While written prior to the rise of e-Commerce most of these principles are relevant to the information exchanged during e-commerce transactions. To avoid unnecessary repetition those relevant to the discussion are identified and summarised in the analysis below.

Milne and Culnan (2004, p.16) suggest that within an e-commerce environment, as well as the normal exchange of money for goods (and associated transactional information), there is another transaction which involves the exchange of personal information for a better quality of service or special offers. This information includes both information willingly provided by the user and other visit-related (traffic) information collected and stored by the site owner or their supplier by the use of non-visible means. In the first exchange the visitor makes a decision whether or not to provide the information, in the second, the visitor is often unaware that the information is being collected and retained. A recent survey of 750 New Zealanders found that 56 percent were concerned about individual privacy. The highest levels of concern were recorded for the security of personal details on the Internet with 84 percent of respondents concerned (New Zealand Privacy Commissioner, 2006).

Privacy statements and privacy seals on websites are both mechanisms used by website owners to provide users with a level of confidence that their personal information will be treated according to a defined "best" practice (Meinert, Peterson, Criswell, & Crossland, 2006, p. 5; Wakefield & Whitten, 2006, p. 3). Papacharissi and Fernback (2005) found that the majority of sites were vague when it came to outlining how personally identifiable information would be protected while "ascertaining their right to collect and trade non-personally identifiable data" A 2001 Harris Interactive survey found that only 3% of adults read the privacy polices on all sites they visit (Peslak, 2005), but they may read them more

often when supplying personal information. For example Milne and Culnan (2004) found that consumers will read notices if they have limited prior experience with a site and were asked to disclose personal information. They found however that the statements only form part of the user's risk analysis strategy. They also found that users did not read statements that were lengthy or difficult to understand. An example of this is where companies write the policy for their own legal protection rather than for the purpose of building customer confidence.

There are 7 registered banks in New Zealand, with five banks holding 85% of the assets in the banking industry (Steele & Craig, 2002). The New Zealand Banking sector is regulated by the Reserve Bank, Securities Commission, Banking Ombudsman and the New Zealand Bankers' Association, amongst others. Banks are therefore subject to their own set of guidelines and a number of different pieces of legislation besides the Privacy Act. When the privacy bill was first introduced, the Bankers Association vigorously opposed it. However once the bill was passed, the association did not cite any great difficulties complying with the Act (Slane, 2001). In fact, the number of privacy complaints in relation to banking since the passing of the Act has been relatively minor. It was reported that in 2000 the Privacy Commission received 30 complaints about the banking industry, which amounted to only 3.5 percent of all the complaints received (Slane, 2001). According to two commentaries by the Privacy Commissioner, the majority of the complaints received concerned with banking related to improper disclosure where security practices were not being practised (Slane, 2001, Slane, 1997). While banks have a number of responsibilities under the Privacy Act 1993, customers also have a responsibility to fully understand what happens to personal information collected about them, as well as take prudent steps to safeguard their cards, pin numbers and account details (Coddington, 2006).

Methodology

The methodology employed in this study was a content analysis. The privacy statements found on the websites of all New Zealand banks were subject to a content analysis comparing them with the provisions of the New Zealand Privacy Act 1993. Those banks analyzed were the Bank of New Zealand (BNZ), Auckland Savings Bank (ASB), National Bank, Westpac Bank, ANZ Bank, Kiwibank, and Taranaki Savings Bank (TSB). Note that the ANZ maintains a separate website from the National Bank even though they have merged, reflecting the ANZ Banking Group's intention to retain the National Bank as a separate brand. General notes were also made about the language and readability of the statements. The analysis was carried out by graduate students as a class project. Only those features substantiated by all students form part of this discussion.

Analysis of New Zealand Bank Privacy Statements

Although the original content analysis identified shortcomings in the websites of individual banks, it is not the intention of this analysis to "name and shame". Rather, this analysis identifies principles within the Privacy Act that are inadequately addressed as indicative of issues for the attention of banks.

Accessibility and language

All of the banks surveyed had some kind of privacy statement, although not all of them were easy to find, the worst being the statement at a minimum of three clicks from the bank's homepage. Naming conventions were variable with some banks using "Privacy Statement",

others using "Privacy Policy", and one "Personal Information Rights Statements" (accessed from a Privacy Policy link). Another bank used the heading "Privacy" for a paragraph under the "Site Terms and Conditions".

Pollach (2006) highlights some areas of concern with privacy statements, in particular the use of language to mitigate the effect of certain policies – examples being the association of cookies with "small", and being frequently used, as well as the use of passive language in order to reduce the apparent effects of some practices. All banks use language in their privacy statements to reinforce the twin concepts of competence and integrity in their dealings with customers. With one exception, all of the bank privacy statements that mention cookies associated them with being small files, common usage, or both. They also use passive language in association with information collection and the use of cookies with positive actions such as providing user preferences and preventing unauthorized access. Two banks used legalistic language that at best would be difficult to read – further reducing the transparency of their privacy statements.

The Privacy Principles

Principle 1 – purpose of collection should be lawful and necessary. It was found that compliance with this principle should be a significant concern for banks

Principle 2 – source of information should be the individual concerned – unless the information is publicly available. Without attempting to identify the customer through tracking the IP address, receipt of email or other means, banks are unable to guarantee that the information they receive comes from the individual concerned. Furthermore, banks use credit reporting agencies to gather personal information, but are required to obtain authorization from the individual concerned. Only three banks advised that they make credit checks two of whom advising that a customer's use of the bank's services constitutes authorization to obtain information from credit providers.

Principle 3 – stating that information is being collected, the purpose of collection, intended recipients, etc. This principle is mainly observed, but some banks did not provide names and addresses of the collecting and holding agencies, method of collection, and what was done with the information. Banks are reliant on customers reading the website privacy statements in order to discover, presumably after the fact, that they are adequately addressing this provision.

Principles 4 – information should be collected in a fair way by fair means. None of the statements addresses this issue and the Banking Ombudsman (2005) makes no reference to complaints about this principle. One must assume that banks would be observing this principle.

Principle 5 – information should be held securely. This is a significant issue for banks. All banks make some sort of statement about holding customer information securely and were considered compliant on this principle. .

Principle 6 – an individual should be able to confirm that the agency holds information about them and access that information. Again all banks offer their customers the right to access personal information held by them.

Principle 7 – correction of personal information. All banks state that customers may request correction of information, but none offer confirmation that correction has been made or that agencies to which information has been disclosed will also be informed, and the information corrected. A minimalist approach.

Principle 8 – accuracy to be checked before use. Only one bank acknowledges the obligation to keep personal information up to date.

Principle 9 – retention of information. This is not mentioned in any of the bank privacy policies. While the Reserve Bank Act of 1989 sets seven years as the limit for retention of certain documents, there is no mention of electronic documents, communications or data. The lack of acknowledgement of this principle by banks may indicate that they do not have an efficient retention and disposal programme.

Principle 10 – information collected for one purpose may not be used for another. The exceptions to this principle are where information is publicly available, or the use is authorized, or that non-compliance is necessary due to legal or public good reasons. Most banks notify customers through their privacy statements that their authorization will be sought before personal information is used for a new purpose or sold to third parties. All banks state that information provided would result in the customer receiving details of other products and services, newsletters, surveys or information. Some banks offer customers an option to opt-out of receiving such information or services.

Principle 11 – disclosure to other agencies. The issue is whether permission has been sought by banks for disclosure to other third parties. Banks rely on disclosure being authorized by the individual or that the information did not specifically identify the individual. With one exception, all of the banks include affiliates or Nielsen/Netratings as recipients of either personal information (in order to provide marketing materials) or non-personal statistical information. The question arises whether customers would be agreeable in all cases for their information to be provided for all the purposes decided by the banks or their affiliates.

Principle 12 – limiting the use of unique identifiers. None of the privacy statements refers to the use of unique identifiers. It is unsurprising that no bank addressed Principle 12 in its privacy statement because there are risks to privacy from using unique identifiers and also from not using unique identifiers. The risk in using a single unique identifier across multiple information collections is that unrelated information about an individual could be used out of context. As it applies to systems for managing information, it is a significant issue at a systemic level for the aggregation of information, rather than being an issue in privacy considerations. However, if IRD numbers or other unique identity numbers are collected as part of the personal information required by banks – as happens in many countries, but not New Zealand – then this could be a problem area for privacy considerations.

Trans-border information flows

All of the New Zealand banks with overseas headquarters have a policy of sharing personal information of New Zealand customers with their overseas-based banking group, but without an explicit commitment to preserving privacy according to New Zealand's Privacy Act. Rose (2006) notes an international trend in legislation against privacy safeguards following on from catastrophic international terrorist events in recent years, and identifies globalization, together with advances in information technology capability as issues of growing concern for information privacy. Slane (1997) sets out the international approaches to maintain privacy safeguards in the face of trans-border information flows. But this adds a whole new level of complexity to the current situation where New Zealand banks have not yet demonstrated that they are addressing the requirements of New Zealand's privacy legislation let alone giving attention to the requirements of other legislations.

Conclusions

This study finds a basic level of understanding and commitment to the privacy of customer information by New Zealand's major trading banks. Although all of the banks had a privacy policy of some description, indicating an attempt in some way to address the issue of customer concerns for privacy, a number did not disclose sufficient detail to allow the customer to make an informed decision about their privacy policies. None of the banks was able to address those more complex requirements that would require sophisticated business processes. Some banks confused information about security of electronic transactions with information about privacy. While appearing to be committed to basic provisions such as the right to view and amend personal information, none of the banks demonstrated through their privacy statements a thorough and pervasive commitment to meeting all the requirements set out in the 12 Privacy Principles. Particularly where this would require a significant investment in strongly controlled business processes, the banks tended to avoid making a policy statement that would commit them to the legal requirements.

One could argue that the principles of the New Zealand Privacy Act of 1993 are a reflection of the privacy values and concerns of the people of New Zealand, tested by wide consultation, approved by Parliament, and forming the basis of human rights considerations. As such, it forms a lens through which one could consider whether internet websites conform to the national values, and therefore a framework for evaluating websites in New Zealand.

Accordingly, one can conclude that the use of privacy legislation principles as a means of evaluating website privacy statements is revealing and convincing. It is considered that increasingly customers will seek assurances from Internet businesses that their confidence is well founded. Business integrity as demonstrated by the provision of comprehensive and relevant privacy statements will go a long way to provide those assurances. The next step is to broaden the investigation to other businesses in New Zealand, and thereafter, if the basic principles remain applicable, to extend it to an international level. While privacy legislation may vary among jurisdictions, there is an international commonality to the principles that would enable worthwhile conclusions to be drawn.

Bibliography

Banking Ombudsman, (2005). Annual Report 2005. Retrieved 14 April 2006 from http://www.bankombudsman.org.nz/documents/BankingOmbAnnualRpt05.pdf

Coddington, D. (2006). Banks... what are they good for? Herald on Sunday. 9 April: p18.

Mason, R. O., Culnan, M. J., Ang, S., & Mason, F. (2001). Privacy in the Age of the Internet. In G. W. Dickson & G. De Sanctis (Eds.), Information Technology and the Future Enterprise (pp. 208 - 238). Upper Saddle River, New Jersey, : Prentice-Hall.

Meinert, D. B., Peterson, D. K., Criswell, J. R., & Crossland, M. D. (2006). Privacy Policy Statements and Consumer Willingness to Provide Personal Information. Journal of Electronic Commerce in Organisations, (4:1), pp1-17.

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy statements. Journal of Interactive Marketing, (18:3), pp15-29.

New Zealand. Privacy Commission. (1994). Information Privacy Principles - Fact sheet No 3. Retrieved 10/04/06, 2006, from //www.privacy.org.nz/people/fact30.html

New Zealand. Privacy Commission. (2006). A summary report. Retrieved 19 April, 2006 from http://www.privacy.org.nz

OECD. (1981) Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data. Retrieved March 3, 2006, from: http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm.

Papacharissi, Z., & Fernback, J. (2005). Online privacy and consumer protection: an analysis of portal privacy statements. Journal of Broadcasting & Electronic Media, (49:3), pp259-282.

Peslak, A. R. (2005). Internet Privacy Policies: A Review and Survey of the Fortune 50. Information Resources Management Journal, (18:1), pp29-41

Pollach, I. (2006). Privacy statements as a means of uncertainty reduction in www interactions. Journal of Organisational and End User Computing, (18:1), pp23-49.

Rose, E. (2006). An examination of the concern for information privacy in the New Zealand regulatory context. Information & Management. (43:3), pp322-335. Retrieved 14 April 2006 from Science Direct database.

Slane, B. (1997). Privacy laws issues - reform proposals and their impact on the financial industry. Fourteenth Annual Banking Law and Practice Conference, Sydney, Office of the Privacy Commissioner.

Slane, B. (2001). Small investment, big return. Australasian Institute of Banking and Finance, Office of the Privacy Commissioner.

Steele, J., Craig, D. (2002). New Zealand. International Financial Law Review, July, pp49-57.

Wakefield, R. L., & Whitten, D. (2006). Examining User Perceptions of Third-party Organisation Credibility and Trust in an E-Retailer. Journal of Organisational and End-User Computing, (18:2), pp1-19.