VICTORIA UNIVERSITY OF WELLINGTON
Te Whare Wananga o te Upoko o te Ika a Maui

Trusting your bank in a digitally connected world - an investigation into perceptions of privacy by bank customers

MMIM 592

by

Shivonne Londt
301023890

Supervisor: Tony Hooper

Submitted to the School of Information Management,
Victoria University of Wellington
in partial fulfilment of the requirements for the degree of

Master of Information Management

09 November 2011

Preface

This report is not confidential.

I certify that the report is my own work and all references are accurately reported.

SHIVONNE LONDT

Abstract

People are placing more of their personal information online as the use of online social networking sites (OSNs) grows. Individuals often lack an awareness around the privacy implications of placing their personal information on these sites but still have an expectation of privacy about this information that may not entirely be justified. OSN data is often used for purposes other than those for which it was provided, but customer demand for ethical and compassionate use of their data is growing. Customers expect greater corporate social responsibility from companies, and especially banks, after the recent global financial crisis. Customers may perceive the use of OSN data by New Zealand banks to influence their lending decisions as a privacy violation.

This study is intended to evaluate whether this use of OSN data would be perceived by customers to be a violation of their privacy. The research was carried out through a web-based survey and follow-up interviews with selected respondents. It was found that the less aware that respondents were about OSN privacy policies, the greater their expectation of privacy. The research also highlighted that even respondents who did not expect their data to remain private still had an expectation of privacy. A lack of perceived control was found to be associated with a greater expectation of a privacy invasion. Trust in respondents' banks was associated with a negative perception of those banks' use of OSN data for lending decisions. This study has revealed a high likelihood that a perception of betrayal coupled with a perceived privacy violation would take place should New Zealand Banks use OSN data in this manner.

Table of Contents

List of Figures

Introduction

The use of online social networking sites (OSNs) is growing worldwide (comScore, 2010, 2011a, 2011b). As a direct consequence of this, people are placing more personal information about themselves online, often without regards for the use to which this information may be put (Chen, Ping, Xu, & Tan, 2009). Coupled with this, it has been found that OSN users generally lack an awareness of the privacy implications of posting personal information, yet still retain an expectation that this information should remain private (Levin & Abril, 2009).

At the same time, the banking environment is becoming more competitive (Boot & Marinĉ, 2008) and banks are looking for ways to obtain a competitive advantage in the market in order to remain financially successful (Srinivasan, Lilien, & Rangaswamy, 2002). Banks in the United States of America (USA) have been using personal data found on OSNs to influence their lending decisions so that they can gain a competitive advantage (Baird & Gonzalez-Wertz, 2011; Finney, 2010). Although banks already have an intensely personal picture of an individual as a result of the data provided when that individual enters into a contract with the bank, there may still be certain areas of that individual's behaviour relevant to lending decisions that are not transparent. Using data on OSNs to complete this picture may thus allow banks to gain a competitive advantage by being able to reduce their risk on lending decisions.

This would not be the first occurrence where data from OSNs has been used for purposes other than that for which it was posted. Canadian police and police at various universities in the USA use Facebook and MySpace to monitor underage drinking (Hodge, 2006; Steeves, 2008). State agencies in the USA are permitted to circumvent individuals' privacy settings on OSNs and access their information to evaluate potential employees under the terms of the Patriot Act (Debatin, Lovejoy, Horn, & Hughes, 2009). Employers are also increasingly using OSNs to perform "informal online background checks" on potential employees and make decisions on their eligibility for the jobs

offered based on what is revealed by these background checks (Clark & Roberts, 2010).

Clark & Roberts (2010) indicate that employers often assume that using OSNs for character checks of job applicants is an acceptable process, especially when considered in the light of “protecting themselves and shareholders”. OSNs allow for these background checks to take place and can reveal the nature of decisions applicants will make in their personal lives and in their jobs. Similarly, banks may feel that using OSNs to perform background checks on potential customers to determine the kinds of financial decisions these customers may make is acceptable when done with the intention of protecting the banks themselves as well as their existing customers (Brandenburg, 2008). Clark & Roberts (2010) propose that, although some OSN users may readily conclude that “what is online is public”, others may not share this view and should not be unfairly disadvantaged because of it. Clark & Roberts (2010) also indicate that the Internet has caused a radical change in the way that people interact and communicate and thus suggest that these sorts of online checks may prevent honest communication online. This could hamper the use of the Internet, and OSNs, as a communications medium by reducing honesty and impeding people’s online interactions.

Coupled with this, there is a growing consumer demand for an ethical and compassionate attitude from companies. Companies are expected to act with “kindness” in their internal operations as well as externally towards customers (Gerzema & D'Antonio, 2011). There is thus a heightened focus on corporate social responsibility and customers are prepared to back this change in attitude with consumer buying power (Gerzema & D'Antonio, 2011; Wagner, Lutz, & Weitz, 2009).

Banks, especially, are under a greater degree of focus for their actions towards customers as a result of the recent global financial crisis (Reynolds, 2010; Worthington & Welch, 2011). Using customers’ OSN data may be seen by those customers to be a violation of their privacy even though it is permissible for banks to use any publicly

available information as a basis for lending decisions under the terms of the New Zealand Privacy Act 1993 (Privacy Commissioner). It is thus necessary for banks to consider this factor before using OSN data in this manner, even though it may grant them a much-needed competitive advantage, because of the potential implications to their reputation and the trust of their customers. Nissenbaum (1998) has, however, acknowledged that in upholding one party's privacy, disadvantages and potential restraints are imposed on others. Upholding individuals' privacy with respect to the data they have placed on OSNs may prevent banks from taking advantage of a potential source for competitive advantage.

This research is not intended to be a philosophical exploration of ethics or the ethical behaviour of banks. It is, instead, intended to be a way of evaluating whether banks' use of data found about customers on public OSNs to improve their lending decisions would be perceived by customers as a violation of their privacy. This research will be presented as an initial critical review of the relevant literature, followed by a discussion of the research methodology used and an explanation and discussion of the findings. Finally, this research will apply the findings to developing a conclusion as to whether a perceived privacy violation could occur from the outlined use of customers' data on OSNs.

Literature Review

Social Exchange Theory

Social exchange theory (SET) indicates that certain "rules" need to be followed in order for relationships to evolve into mutually trusting and loyal relationships (Cropanzano & Mitchell, 2005). Relationships are based on a comparison of the costs and benefits of the relationship and, should it not be considered satisfactory in this context, then this will result in an evaluation of alternatives to the relationship (Richardson, 2001). The costs of the relationship are weighed up against the benefits to determine the relationship's worth and this outcome is then evaluated against the individual's expectations in order to determine the level of satisfaction with the relationship (Luo, 2002). If the relationship is not deemed satisfactory and there are preferable alternatives available, this reduces the individual's dependence on the relationship and vice versa. Luo (2002) also indicates that SET considers trust to be a key component in building relationships.

Thus, according to SET, when a customer of a bank considers the situation where the bank may use that customer's OSN data to influence lending decisions, the customer will weigh up the potential costs and benefits and will consider the potential for alternative relationships, namely other banks. An individual with a strong dependence or attachment to their bank may thus find it difficult to consider moving banks even though they consider the use of their OSN data to be a betrayal of their trust and a violation of privacy. Similarly, an individual may feel that these costs do not actually outweigh the benefits of remaining in a relationship with this bank and would thus not consider leaving, despite the perceived betrayal or privacy invasion. Of course, the individual may not perceive these costs to be present at all as the determination of costs and benefits in a relationship is highly subjective (Emerson, 1976).

Communication Privacy Management Theory

Communication privacy management theory (CPMT) deals with the way in which individuals control access to their private information (Petronio, 2007). It introduces the

concept of “boundaries” to separate public information from information perceived as private (Bateman, Pike, & Butler, 2011; Child & Petronio, 2010). The “permeability” of these boundaries, or the degree to which information can flow through them, changes depending on the type of relationship and information being communicated (Child & Petronio, 2010). CPMT indicates that there are both risks (increased vulnerability) and benefits (a potential for a deeper relationship through greater intimacy) in revealing private information. It also deals with how individuals manage revealing and concealing information in communications. If private information is shared, the party with whom it is shared becomes a co-owner of the information and has certain rights and obligations in terms of it, including how it can be used and to whom it can be revealed (Bateman, et al., 2011; Petronio, 2007).

CPMT also introduces the concept of “boundary turbulence” where the rights and obligations around shared information are not clearly understood by the co-owners of the information or when one of the co-owners violates these boundaries (Child, Pearson, & Petronio, 2009; Child & Petronio, 2010). This makes the original owner more wary of revealing information to the other party in the future, thus impacting their trust of that party.

Context is also an important concept in CPMT. Depending on the context, individuals may be willing to sacrifice a certain level of privacy in order to achieve specific goals (Child & Petronio, 2010), such as the potential to expedite the granting of a loan through better data collection practices by banks.

In the situation being considered here, placing information on OSNs can be considered to be a form of communication (Pike, Bateman, & Butler, 2009). According to CPMT, banking customers will feel that certain boundaries apply to the information they have revealed on OSNs. Although they may consider the information to be in the public domain, it is likely that they consider people who access the information to have certain obligations around its use. A violation of these boundaries could impact the relationship, if any, with the party who violated the boundaries, thus potentially harming the

relationship between the customer and the bank. As SET indicates, this may result in an unacceptable cost in terms of the relationship and may cause the customer to start considering alternative relationships with other banks.

Research Model and Hypotheses

Expectation of Privacy

Privacy has been defined as "the ability of the individual to control the terms under which personal information is acquired and used" (Westin, 1967). Privacy can also be considered to be the personal information that an individual sees as important to themselves and as inaccessible by the general public (Timm & Duven, 2008). It further includes the right of that individual to control the distribution, as well as the use, of this information (Berman & Bruening, 2001). Hodge (2006) indicates that there are two main issues to bear in mind when considering the subject of privacy, namely:

- the intent behind sharing the information; and
- the expectation of the individual that the information would remain private.

OSNs by their very nature facilitate the "rapid and widespread dissemination of personal information" (Levin & Abril, 2009). Users of OSNs share personal aspects of themselves with others, who may not necessarily be the intended recipients of this information, which allows for a connection to be established back to the user's offline persona and life (Bateman, et al., 2011; Lenhart, 2009). According to CPMT, this has the unintentional effect of reducing the permeability of the barriers around a user's private information. This may result in conflicting expectations around the privacy of individuals' information.

OSNs also result in the establishment of a permanent and indelible record of an individual's actions there (Nissenbaum, 1998). Even if individuals delete information, it may be cached on servers or retrieved through search engines (Clark & Roberts, 2010). OSN users may thus lose control over the information they have shared where the parties who can access this information may not necessarily use it in a benign manner

(Ware, 1984). This has an impact over an individual's expectation of privacy as it reduces the individual's control over their personal information.

As Chen, et al. (2009) indicate, however, the concept of privacy in the "online social context" (OSC) is quite different to privacy in an "online commercial context" (OCC), such as e-commerce or online banking. In the OCC, privacy is generally well regulated. Customers have greater control over their personal information and can request to be provided with the personal information that a company holds on them. Similarly, they can request that this information be updated or even removed from a company's records under certain circumstances. In the OSC, privacy is less well defined as evidenced by frequent changes of privacy policies within certain OSNs (The Telegraph., 2011) and the lack of control over the information that contacts within these OSNs may post about other individuals (Dwyer, Hiltz, & Passerini, 2007).

It is thus necessary to consider whether an individual would have a reasonable expectation of privacy with regards to their OSN data given the largely public nature of OSNs. It is also necessary to consider whether a bank's use of this data is thus a violation of a customer's privacy.

Meredith (2006) and Hodge (2006) contrast the difference in privacy expectations in posting information on OSNs with the intention of making it available to others, and in actively manipulating privacy settings on OSNs to limit access to the posted information. In the first instance, the information cannot be expected to be kept private as the intention was to share the information publicly. In the second instance, however, an individual has a reasonable expectation of privacy. Meredith (2006) emphasises that it is still the *choice* of the individual to post the information. They are not compelled to do so. As Butterworth (2008) indicates, though, privacy is about the expectation of whether information is private, rather than whether someone has "done or said something in public".

Awad & Krishnan (2006) indicate that knowledge is a determinant of perceived control of an individual's personal information. It is therefore reasonable to assume that an individual's knowledge of the privacy policies of the OSNs in which they are involved will influence their expectation of privacy.

Hypothesis 1: Individuals' expectation that the data posted on OSNs will remain private will be influenced by their awareness of the privacy policies of the social networking sites.

Nissenbaum (1998) indicates that there is little or no "reasonable expectation of privacy" in the public arena, especially if the information is shared voluntarily in public. Users of OSNs, however, may have a different expectation. Levin & Abril (2009) introduce the concept of the "privacy contradiction" where users willingly disclose personal information on OSNs but still retain an expectation of privacy. Bateman, et al. (2011) also highlight the potential conflict that occurs where OSN users are required to reveal a certain level of personal information in order to take part in the OSN community but do not necessarily want this information to become public to "an unknown audience".

Many people thus consider the information posted to OSNs to be private or believe that it should be private (Hodge, 2006). Most social interactions that take place offline leave little or no record of their occurrence but the same cannot be expected for online interactions on OSNs (Dwyer, et al., 2007). Web technologies and the Internet are considered to have changed the concept of "publicness" (Bateman, et al., 2011). Slevin (2000) indicates that, in order for something to be public, it no longer requires individuals to be "in the same space at the same time", but can be made public through the use of information and communication technology and thus be made visible and accessible to other people. This may not, however, be apparent to OSN users, who do not have an immediate awareness or visual clues that others are present and can access their information (Bateman, et al., 2011). This could thus lead to a false expectation of privacy on OSNs.

Although individuals may expect a degree of privacy based on their privacy settings on OSNs, information posted by their contacts on these sites may not be subject to the same expectations (Dwyer, et al., 2007). Information posted by an individual's contacts on OSNs may also cause embarrassment or harm to that individual if viewed out of context (Dwyer, et al., 2007). There is also a growing concern that friends may intentionally or unintentionally post personal information about OSN users without their consent (Chen, et al., 2009). In addition, some information posted on OSNs may not actually be subject to individuals' privacy settings. Facebook, for example, indicates that comments and other information posted to Facebook Pages are considered to be public, publicly visible and able to be used by the Page owner outside of Facebook (Facebook, 2011). OSN users may often not be aware of these variations in privacy policies, especially if they have not read the terms and conditions of the OSN sites, and this may affect their expectation of privacy with regards to their data.

Brandenburg (2008) indicates that "being seen by some does not mean one should be seen by all". This implies that placing information on an OSN to be viewable by a select group should not compromise an individual's expectation of the overall privacy of this information. Brandenburg (2008) also suggests that if an individual has taken measures to protect their data, for example by applying the privacy settings that the OSN offers, then that individual is more deserving of privacy than one who has not.

Hypothesis 2: Individuals will have an expectation of privacy regarding the data posted to OSNs, regardless of the privacy settings of those sites.

Providing control, or the illusion of control, over the privacy of an individual's information can also influence an individual's expectation of privacy (Barnes, 2006). As Barnes (2006) indicates, OSNs often provide a variety of both access and privacy control measures, such as the requirement to enter verification details in order to log into a site or the ability to close certain information off to predefined groups of users. These measures may give a greater perceived control over an individual's privacy and thus reduce the expectation of a privacy invasion.

Awad & Krishnan (2006) also indicate that the level of control that an individual perceives they have over their data can also influence their expectation of privacy on an OSN. Control can be seen to be provided through an individual's privacy settings on the OSNs on which they participate. As Awad & Krishnan (2006) indicate, the greater the individual's control over the privacy of their information, the less that individual will be concerned over potential privacy invasions.

Hypothesis 3: The greater the perceived control an individual has over their OSN privacy settings, the less the expectation of a potential privacy invasion

Trust

Reynolds (2010) indicates that the finance industry has recently been negatively impacted through "unwise and unethical decision making" around mortgage approval and credit extensions. Customer confidence in the entire finance industry in New Zealand, which includes the banking industry, has dropped to the lowest level since the Financial Confidence Index was launched in 2009 (RaboDirect., 2011). Morgan & Hunt (1994) indicate that confidence forms a basis for trust so this loss of confidence can be extrapolated to include a loss of trust by consumers in banks themselves.

Trust is comprised of competence, benevolence, integrity and predictability and has been defined as a belief that another party has characteristics that may be "beneficial to oneself" (Dimitriadis, Kouremenos, & Kyrezis, 2011). Of interest to this research are the aspects of *benevolence*, which consists of a belief that the other party will act in one's best interests, *competence,* a belief that the other party is capable of doing what needs to be done in a given situation, and *integrity*, which involves a belief that the other party will act ethically (Dimitriadis, et al., 2011). The major New Zealand banks have emphasised their intentions to act ethically and in the best interests of their customers on their publicly accessible websites (e.g. ASB Bank Limited., 2011; KiwiBank., 2011b; The National Bank of New Zealand., 2011a; Westpac New Zealand Limited., 2008).

Thus it is proposed that the greater the trust that a customer has in their bank, the less they will expect their bank to make use of the customer's personal data on OSNs.

Hypothesis 4: Individuals' trust of the bank of which they are a customer will influence their trust in that bank's use of customers' data on OSNs.

Mayer, Davis, & Schoorman (1995) define trust as "willingness of a party to be vulnerable to the actions of another party based on the expectations that the other one will perform particular actions important to the trustor, irrespective of the ability to monitor or control the other party". As Cazier, Shao, & St. Louis (2006) emphasise that online transactions put the buyer in a potentially vulnerable situation, so does an individual's interaction with their bank put them in a similarly vulnerable situation. Customers are thus placing an enormous amount of personal information into the hands of the bank and placing a lot of trust that the information will be used with discretion, with processes to ensure that banking products can be obtained fairly.

Caldwell, Davis, & Devine (2009) have indicated that a feeling of betrayal results when an expected behaviour associated with an individual's trust is not followed. Betrayal may be either intentional or unintentional and it is entirely likely that the banks have not considered that these actions may result in feelings of betrayal by their customers.

Banks hold a position of power with respect to their customers due to the nature of their business and the information that they hold about individuals (Easterbrook & Fischel, 1993). Despite the recent erosion of trust towards the banking industry in general, customers will largely still trust their banks. They would not otherwise loan money from them or invest with them as this would cause cognitive dissonance, or the psychological discomfort that arises from holding conflicting beliefs about a particular concept (Festinger, 1957). Because of this position of power and the trust that customers hold in their banks, the situation arises where customers could feel betrayed by the actions of their primary bank (Caldwell, et al., 2009).

In terms of Hypothesis 2 above, customers will largely expect the data that they place on OSNs to remain private to those OSNs, and not be used without their express permission and consent. Customers would thus not expect their banks to make use of this data and could thus feel betrayed by banks' use of this data thus resulting in a perceived violation of privacy.

Caldwell, et al. (2009) outline five characteristics of betrayal in a corporate sense, namely:

- betrayal is *voluntary* in that a customer chooses to feel betrayed in particular circumstances;
- betrayal is a violation of expectations that are *pivotal* to the nature of the relationship between the customer and their bank;
- both the bank and their customers are *aware* of these expectations. Banks are largely aware of these as evidenced by the privacy statements of their publicly accessible websites (e.g. ASB Bank Limited., 2009; KiwiBank., 2011c; The National Bank of New Zealand., 2011b; TSB Bank Limited., 2009). These expectations may not always be reasonable, however, as banks are permitted to make use of publicly available data (Privacy Commissioner);
- the expectations of the customer are violated through the *behaviour* of the bank; and
- the customer perceives that the betrayal has the potential to *harm their wellbeing*.

Hypothesis 5: If a customer feels that a bank has betrayed their trust with the use of that customers' data on OSNs then that feeling of betrayal will result in a corresponding perception of a violation of that customer's privacy.

Philosophical approach

A post-positivistic and relativistic approach will be taken by using the analysis of the outcomes of the survey and the interview questions to infer generalisations around the research question (Onwuegbuzie, Johnson, & Collins, 2009). Post-positivism considers that there is an independent, individual reality that can be studied but that, due to cultural backgrounds, researchers will always have a certain amount of bias in their

views of this reality so that they cannot be completely impartial in their observations or interpretations (Onwuegbuzie, et al., 2009). Relativism indicates that the research is influenced by culture in which the research takes place (Bloland, 1989), which will affect the expectations of privacy and basis for trust in individuals' primary banks.

Constructivism, closely related to relativism, views knowledge as being constructed through experience and the relationship with the world through prior knowledge and other people's experiences (Ryder, 2008; Talja, Tuominen, & Savolainen, 2005). This highlights a potential bias in that the interpretation of the survey and interview data will be influenced by personal expectations of privacy and experiences with OSNs.

Methodology

Web Based Survey

The survey questions were constructed from a review of the literature around privacy and privacy issues on OSNs, as well as the literature on trust as it relates to banks. Targeted respondents who are currently customers of the major banks in New Zealand (ANZ, The National Bank, Westpac, ASB, BNZ, Kiwibank and TSB) and are also currently participating in one or more OSNs were invited to take part in the survey and subsequent interview. The survey aimed to get at least ten responses from customers of each bank, thus looking to achieve at least seventy responses in total. Invitations to participate in the survey were sent out to key contacts and colleagues in the banking industry, as well as to postgraduate students at Victoria University.

Schonlau, van Soest, Kapteyn, & Couper (2009) indicate that the survey methodology used will affect the likelihood of including certain demographics of respondents in the survey. Web based surveys thus require all respondents to have Internet access in order to be able to complete them. Because this study focuses on a sample that uses OSNs, they would be required to have Internet access in some form to participate in OSNs. This makes a web-based survey a suitable method to access this sample.

The survey was thus constructed as an online survey. Invitations to participate in the survey and subsequent interview were sent out via email. The survey questions were measured against a five point Likert scale, with potential responses ranging from Strongly Disagree to Strongly Agree, aside from where otherwise indicated. No personally identifiable information was collected from the survey.

The survey questions have been supplied in Appendix 1.

The surveys also collected certain demographic information around the banks of which the respondent is a customer and the OSN(s) in which the respondent participates. Limited individual demographic information was collected in order to contrast responses between genders and ages.

Interview

Interviews were conducted with selected respondents who agreed to be interviewed as a follow-up to the survey. One customer from each of the major banks, aside from TSB which was not represented in the survey responses, was selected as an interviewee. These interviews were conducted as semi-structured interviews and all interviewees were asked the same set of questions. The interviewees were allowed to phrase their answers in their own words rather than pick them from a predefined set of responses (Valenzuela & Shrivastava, 2002). The interviews were recorded and transcribed and interviewees were asked to check the accuracy of the transcripts. A content analysis was then performed against these transcripts. The results of the interviews and subsequent content analysis were reviewed and compared with the results of the survey.

The interview questions are provided in Appendix 2.

Analysis & Interpretation

Analysis

Survey

The questions on privacy were used to build up an overall picture of the respondents' expectations of privacy. This was then compared with the results of the questions on trust to determine the correlation between the expectation of privacy and the individuals' trust in their primary banks. The responses to individual questions were also analysed and common factors identified.

Content Analysis

A content analysis was performed on the interview questions. The analysis was on the latent content as the underlying symbolism of the data was analysed to relate the data back to the proposed model (Schmeck, 1997).

The data was analysed using grounded theory analysis, using the three steps as outlined in (Punch, 2005):

- basic conceptual categories will be found in the data at the first level of abstraction;
- relationships between the categories will be determined; and
- the relationships will be conceptualised and accounted for at a higher level of abstraction.

The data from the open-ended questions from the interview were analysed using a qualitative, open coding method through devising abstract themes as they arise in the content (Punch, 2005) through a framework devised by personal judgement. Common statements around interviewees' perceptions of privacy and trust were identified in the initial sweep of data. The data was also reviewed for consistency with the survey responses. According to Punch (2005), subsequent sweeps aggregated these indicators into the first and second order concepts and patterns by reviewing the responses for common themes and phrases around interviewees' perceptions of trust

and privacy. These concepts were then applied to the findings from the survey in order to gain a greater understanding about the reasoning behind respondents' reactions.

Interpretation

Web-based Survey

One hundred and twenty four completed responses from the survey were received. Two of these responses were discarded due to invalid data. Of the respondents, 56% were male and 44% were female. Ages of the respondents ranged between 21 and 64, with the average age of the respondents being 36. This is indicative of the largely student-based population for the research. The largest subset of respondents was from The National Bank, with ANZ having the fewest respondents. The response from The National Bank can be attributed to students having accounts with The National Bank due to its proximity to Victoria University, as well as the responses from colleagues in the banking industry.

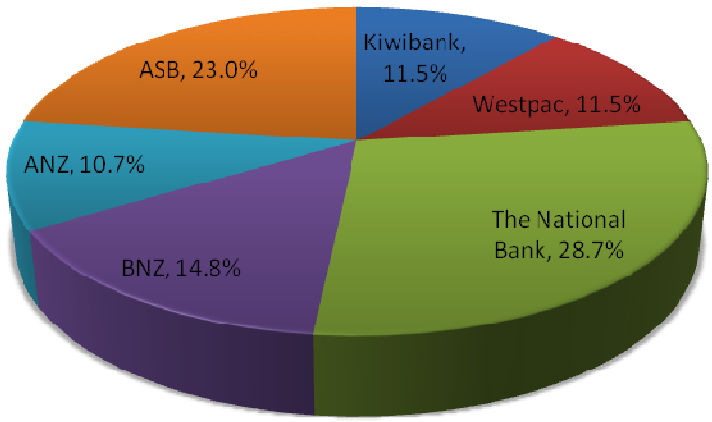

Figure 1: Division of respondents amongst banks

This introduces a bias in the data as customers of The National Bank were over-represented. In order to eliminate this bias, a baseline for the data was established by selecting the bank with the fewest respondents, namely ANZ, and randomly selecting the same number of respondents from the other banks. This ensured that customers

from each of the major banks that responded to this survey were evenly represented. The original data has been provided in Appendix 3.

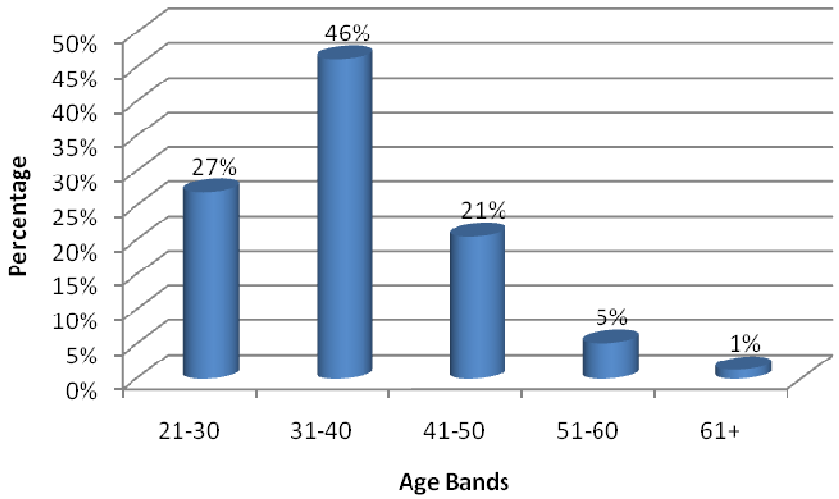

Figure 2: Age bands of respondents from baseline established for data

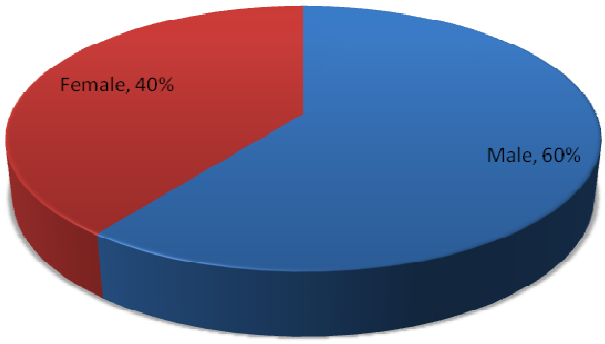

Figure 3: Gender division of respondents from baseline established for data

The majority of respondents participated in Facebook, which is to be expected as Facebook is considered to be the world's largest OSN (The New York Times., 2011). More than half of the respondents also used LinkedIn, which is an indication of the largely professional nature of the respondents. Respondents were able to indicate their participation in more than one OSN.

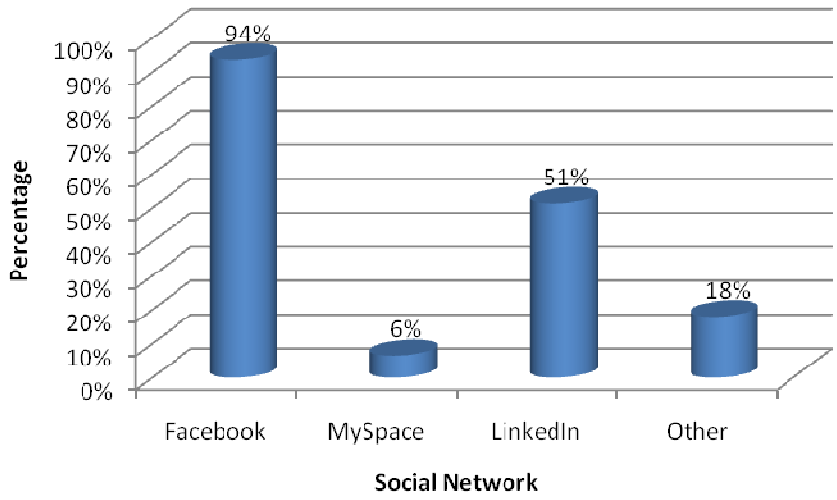

Figure 4: Respondents' participation in online social networks

Privacy

As illustrated in Figure 5 below, most respondents considered themselves to be aware of the privacy policies of the OSNs in which they participated. Of these respondents, the majority had actually read the privacy policies of these sites, thus contributing to this awareness. This raises the possibility for those respondents who did believe they were aware of the privacy policies to have built up this awareness from other sources that may not necessarily be accurate. This may then result in correspondingly false expectations around the privacy of their data. Of those respondents who believed that they were not aware of the privacy policies, almost all had not read them, which could account for this lack of awareness.

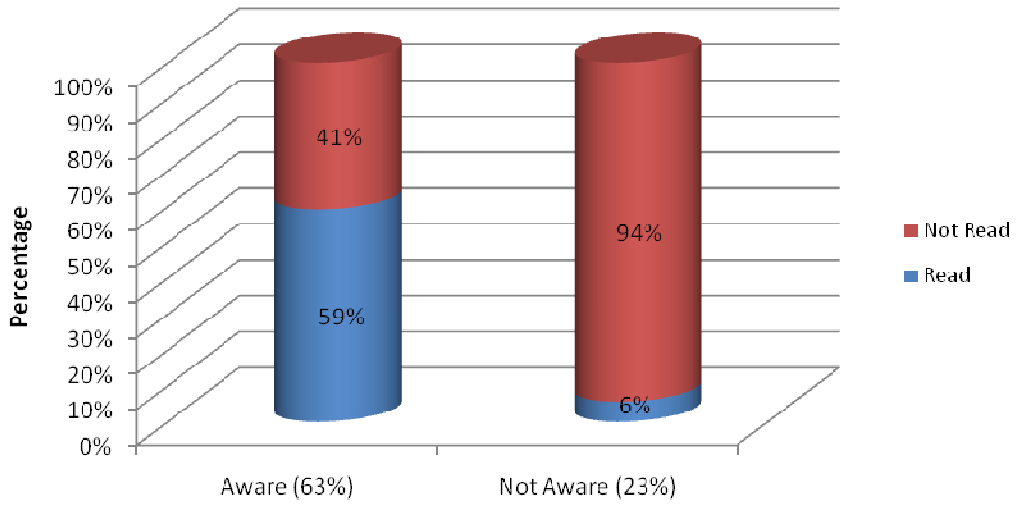

Figure 5: Contrasting awareness of privacy policies with respondents who have read privacy policies

Slightly more of the women than the men had read the privacy policies as illustrated in Figure 6. Fogel & Nehmad (2009) suggest that women tend to be more risk-averse and have greater privacy concerns than men. Reading the privacy policies could thus indicate a desire to be certain of what the privacy policies actually contain as well as a need to ascertain exactly how the individual's privacy may be affected.

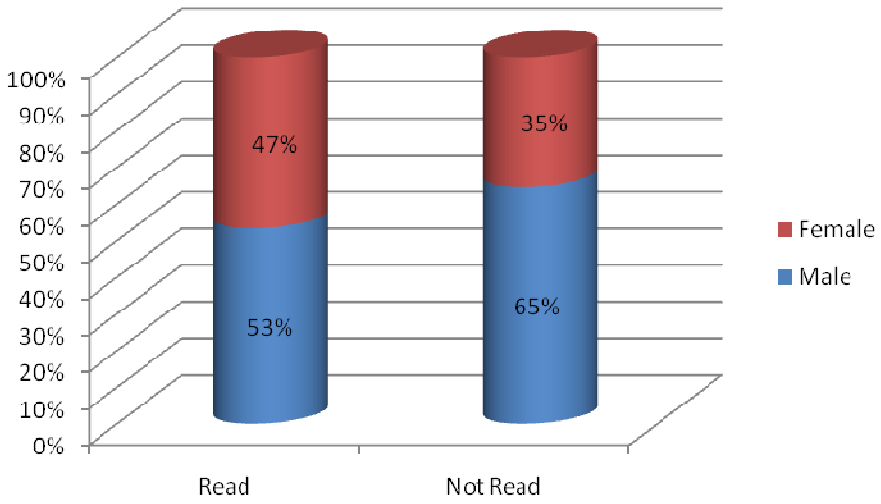

Figure 6: Comparison of whether respondents have read privacy policies by gender

Figure 7 shows the comparison between respondents who believed that information posted to OSNs would remain private to those sites and respondents who did not. Almost half of the respondents did consider that their information would remain private. Less than two thirds indicated that they were aware of the privacy policies of the OSNs but the majority of those respondents had not actually read them. This may have led to a false expectation of privacy. Almost three quarters indicated that they were concerned about third parties accessing and using their data. This appears to be contrary to their expectation that their data would remain private.

Where respondents indicated that they did not expect their information to remain private, almost two thirds had not read the privacy policies. This may indicate a certain level of self-awareness that not reading the privacy policies could have an impact on their expectation of privacy. Fewer respondents in this subset indicated that they were concerned about third parties accessing and using their data. This could indicate that, because this set of respondents does not expect their information to remain private, they have taken steps to either limit the information they place online or ensure that third parties would get no valuable data from their information, thus leading to a reduced concern.

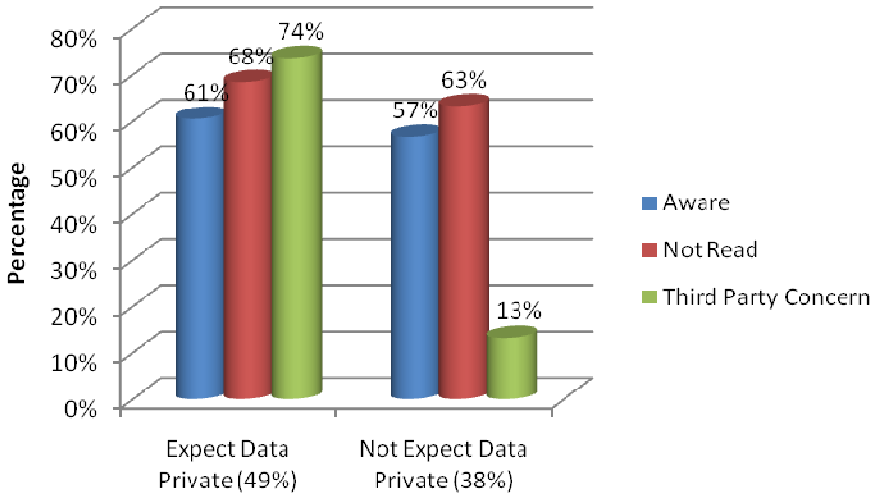

Figure 7: Comparing awareness, reading of OSN privacy policies and concern over third party access of data between respondents who expect their data to remain private and respondents who do not

As shown in Figure 8, most respondents indicated that they believe that the information placed on these sites is publicly accessible. The majority of these respondents were also concerned that their data may be accessed and used by third parties and that they were not able to control the use to which their information may be put. This highlights that boundary turbulence may be occurring, where there is a perception that the boundaries around the control and use of respondents' information are not clearly understood by all parties accessing the OSN data.

Where respondents indicated that they did not believe their information was publicly accessible, a significant portion still indicated a concern over third parties accessing and using their information. None of these respondents strongly disagreed with this question. Similarly, these respondents also indicated that they did not believe that they have control over the use to which their information may be put. This indicates that, even though these respondents do not believe their information is publicly accessible, there is still a concern that the privacy of their information may be violated in some way.

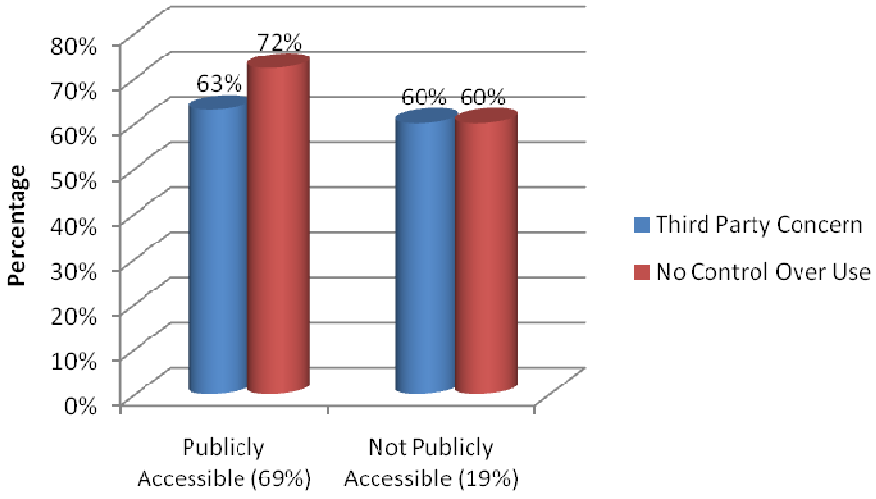

Figure 8: Comparing concern over third party access of data and perception of lack of control over use of data between respondents who their data to be publicly accessible and respondents who do not

A significant proportion of respondents (91%) indicated that they believed that the data they place on OSNs leaves a permanent trace of their actions there. No respondents strongly disagreed with this question. This indicates a high level of awareness of the permanence of the information placed online as raised by Nissenbaum (1998). As the target group is largely professional in nature or involved in post-graduate studies and thus well educated, this would account for this accurate perception.

The majority of respondents did not believe that they had control over the privacy (53%) or the use of their information (68%), with more of the male respondents having this perception, as illustrated in Figure 9. Because of the increased privacy concerns that women have been found to have with regard to their OSN data (Fogel & Nehmad, 2009), this may indicate that the female respondents have taken greater measures to ensure the privacy of their data.

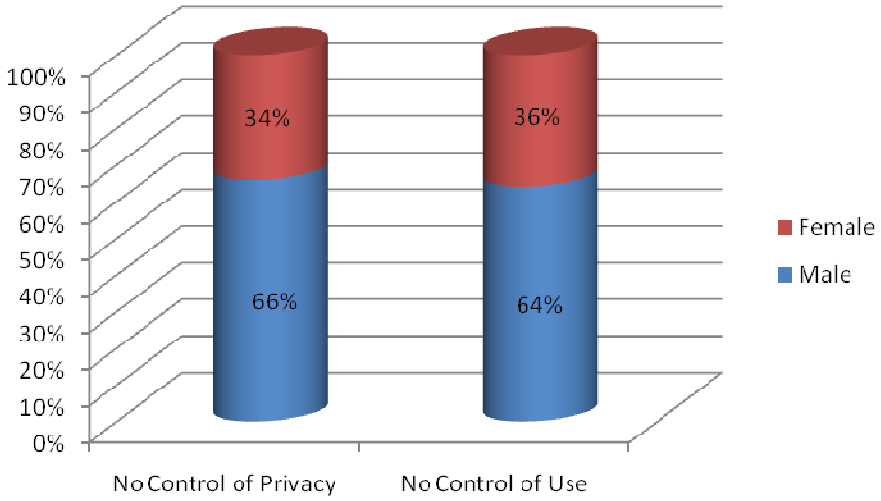

Figure 9: Comparing perceptions of a lack of control over privacy and use of OSN data by gender

Trust

Fewer than half of the respondents (47%) believed that their bank looks out for their best interests. The largest subset of these respondents was from Kiwibank, as shown in Figure 9. Of the respondents who did not believe their bank looks out for their best interests (33%), the largest subset of respondents was from ASB. Kiwibank has won

awards for its performance and for customer's trust since 2007 (KiwiBank., 2011a), which could account for a legacy of trust amongst respondents from Kiwibank. ASB ranked 6th out of the major New Zealand banks in the 2011 Bank of the Year Awards (O'Neill, 2011), which could account for the perception amongst respondents that this bank does not look out for their best interests.

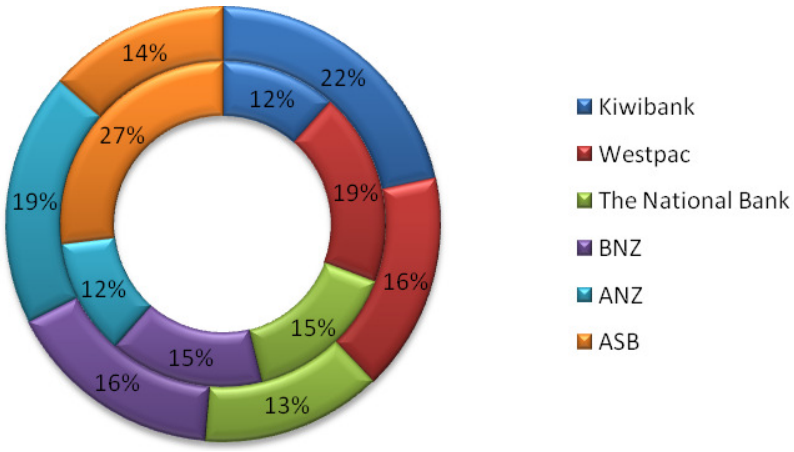

Figure 10: Comparison of percentage of respondents who believed their bank looks out for their best interests (outer circle) and respondents who do not (inner circle) by bank

The majority of respondents believed that their primary bank was competent in the actions they take around lending decisions (74%) and that they had integrity in these actions (68%). No respondents strongly disagreed with either of these statements. This indicates a high level of confidence amongst respondents in banks' actions around lending decisions.

Less than half of the respondents believed that their primary bank was aware of the obligations around their use of respondents' OSN data (45%) but more than a third of respondents were undecided (38%). As banks in New Zealand have only recently started to engage with their customers in the OSN space, it may indicate that many respondents have not considered this previously or that banks have not done enough to promote their awareness to these respondents in this space.

The majority of respondents (63%) believed that their primary bank has an obligation **not** to use any data not explicitly provided to them, with the greatest subset of respondents (31%) strongly agreeing with this statement. This highlights that respondents have strong feelings about this issue. As indicated previously, however, banks are entitled to make use of any publicly available information about their customers or potential customers. This may result in a potential conflict for banks over this issue. None of these respondents strongly disagreed with this statement.

The majority respondents (56%) believed that the use of data from OSNs by banks to influence their lending decisions had the potential to cause them harm. This may imply an inherent awareness amongst these respondents that the information they are posting to OSNs is of a compromising nature, depending on who can access it.

Interview

Interviews were held with six respondents (two male and four female) from the web-based survey who indicated their willingness to take part in the follow-up interview. One respondent from each of the major banks was chosen. Significant responses to the interview questions are provided in the table below. Respondents are identified by the letters A to F.

1. What are your expectations around the privacy of the information that you place on social networking sites?				
A: I think it's mainly the responsibility of the user	B: That my details that I don't want other people to see are not disclosed to other people or organisations	C: I am, personally, quite wary about what I put on there and, if it's a message to someone, I kind of write it in code	E: I understand that different companies and stuff can access the information – which I find I'm uncomfortable about	F: I think the majority of users don't understand the basic business model behind most social networking environments and don't appreciate that their information is not there for their benefit

2. What are your concerns around the privacy of the information that you place on social networking sites?		
A: It is that they'll be used for slightly devious means. Personally I put things on social networks that I'm not concerned about people seeing anyway.	B: My main concern is almost that I don't understand the privacy settings and the implications.	C: I must admit I haven't read the fine print.

3. What are your opinions on the fairness of banks using data from social networking sites to influence their lending decisions?			
A: That's going very much into your private life and you as a person, not how you deal with your finances so it's a fairly grey area I think at this stage.	B: I expect them to respect whatever privacy settings are for the users. On the other hand I've also been thinking I expect my bank to go out proactively and find out if they're lending money to someone, or me, or whoever, that they proactively go out and find is this a person that can be trusted because I don't want my bank to lend a lot of money to someone who is not trustworthy.	C: I wouldn't feel very happy about it.	E: I wouldn't be comfortable with a bank deciding my lending based on what it said on Facebook.

4. What are your perceptions of your primary bank as a benevolent entity?
B: It is a business and I think that they should be run as a business but still with a concern for their customers. I don't expect them to take care of me and so on. I expect that that should be people's own responsibility.

5. What are your expectations around banks' use of your data from social networking sites?	
C: I certainly wouldn't be ever expecting them to be tracking my social web presence.	B: I'd hope that whatever they found in that situation that they'd treat it with a bit of … you know … be wise about it.

6. How does your trust of your primary bank influence the fact that they may use your publicly accessible data from social networking sites to influence their lending decisions?		
A: Again, if it was for that risk assessment side of things and it was to make a call on that then I guess there's a reason for it. If they use that beyond those types of things then I think it's actually quite unethical.	C: I would just move banks to a bank that said they didn't unless they could show me proof somehow that what they're doing is going to benefit me in some way.	D: It would make me lose trust in them I think or make me think they're a bit dodgy.

7. If you have any other comments to make, please state them now.	
A: Occasionally I cringe at what some people put up because it's not that private and, once it's there, it's there forever and people, I think, do forget that.	B: I see the bank as a business and they're looking out for their own business.

Figure 11: Significant responses from interviews with respondents

Expectation of Privacy

Interviewees largely expected their privacy settings on OSNs to be honoured. There was an expectation that, if their information was locked down through these settings, that this would be respected. Interviewees did, however, perceive that third parties may be able to access some information based on the terms and conditions of the OSNs.

Privacy was thus largely expected on a personal level *between* participants on the OSNs but there was a concern that third parties may have a greater level of access to that information. This was emphasised if users of the OSNs had not read the “fine print” of the terms and conditions. Several interviewees indicated that they were wary of what they posted onto the sites because of this, either “writing it in code” or just not putting private information on those sites. Overall, this indicates a low expectation amongst interviewees that their data is private.

Most interviewees were aware that terms and conditions of the OSNs may impact their expectation of privacy for their data but were aware that, by accepting the terms, they may be impacting the privacy of their information. Several interviewees commented that many people appeared not to “actually take the time to figure out what the terms are”. Only two of the interviewees had actually read the terms and conditions and most interviewees did not consider themselves to be aware of the privacy policies of the OSNs in which they participated. Many interviewees indicated that they felt other people may be less aware of these terms therefore indicating that they expected other people to have a higher expectation of privacy than was warranted. One interviewee commented that users would be unaware that the information they place on OSNs is, ultimately, “not there for their benefit”.

Concerns over Privacy

Most interviewees indicated that they considered the information that they placed on OSNs to belong to them in that it was their “information to share”. They were, however, concerned that third parties may be accessing this information and were concerned that third parties may be using this information for “slightly devious” means, such as background checks. One interviewee also raised a concern over the implications of the privacy settings and what that meant for the privacy of the data on the OSNs.

Overall, interviewees were concerned about the privacy of their information and thus potential privacy violations. Concerns were also raised about their information being used for means other than those for which it was posted online.

Fairness of banks using OSN data

Interviewees' opinions were evenly divided around the fairness of banks using data posted on OSNs to influence their lending decisions. Those interviewees that considered it unfair raised issues around the potential for misuse of the information by the banks, including the fact that the information may be taken out of context or that banks "can misinterpret it". One interviewee also raised the issue that having banks looking at the data placed on OSNs could impact the way that the site was used, as it was primarily a "social kind of outlet where you'd say unprofessional things at times". This confirms Clark & Roberts' (2010) suggestion that using OSNs to conduct background checks will change users' actions and behaviours on them and will have a negative impact on them as a communications medium.

One interviewee also raised the issue that, although they would feel "annoyed" should their bank conduct these sorts of online checks, OSN users should also be aware of what they are posting online and should be cautious when posting information that could have a negative connotation.

Within those interviewees that felt it was a relatively fair use of information, there was still the concept that banks had a responsibility to disclose this to the customer up front and to respect any privacy settings that were applied to the information.

Perception of bank as a benevolent entity

Most interviewees did not consider their banks to be benevolent entities.

For the single interviewee who did indicate that they perceived their primary bank to be a benevolent entity, there was still the acknowledgement that the bank was a business and would ultimately seek to make money and to make a profit. This did not appear to impact their trust for their bank or perceptions of benevolence, however.

The interviewees who indicated that they did not perceive their bank to be a benevolent entity did not necessarily experience reduced trust for their primary bank because of that perception. Rather, it was an acknowledgement that the bank was run as a business and that, in that context, they considered their bank trustworthy as long as they operated within the legal and regulatory framework of the country in which they operate.

Expectations around banks' use of data from OSNs

Interviewees expressed a variety of opinions around their expectations of banks' use of data from OSNs. Most expected that their banks would use the information if it was available but some felt that the possibility of this use should be disclosed up front. Two interviewees, however, felt that the bank would not use data from OSNs. One felt that it would provide no additional value to them and the other felt that they would not use it because it is not accessible to them due to individuals' privacy settings. One interviewee felt that this would be a questionable given the fact that using OSN data reveals an individual on a personal level, rather than just how they deal with their finances.

Interestingly, one interviewee indicated that, although the bank may make use of OSN data, they would expect the bank to "be wise" and use discretion about the information found online, especially if users post negative information about themselves online. This echoes Edwards & Kleiner (2002) who indicate that employers conducting background checks should not "invade the privacy of an applicant more than necessary".

Influence of trust on banks' use of OSN data

Responses were varied around the question on the influence of trust on banks' potential use of OSN data. There was no connection between trust (or lack of trust) and the perceived use by banks of OSN data. For certain interviewees, a lack of trust for their primary bank meant that the concept that their bank could use their OSN data was entirely repugnant and would result in them "moving banks to a bank that said they didn't". Similarly, amongst those interviewees who did trust their primary bank, one

indicated that they had no issue with their bank using their OSN data in this manner. Another interviewee, however, indicated that, although they currently had high trust for their bank, the use of their OSN data in this manner would cause that interviewee to lose trust in their bank.

Discussion

Hypothesis 1

Respondents' expectation of privacy (EP) was measured by the following question:

- I expect that the information posted on these sites will remain private to the sites themselves.

If respondents have either agreed or strongly agreed with the above question, they are considered to have a high EP.

Perceived awareness of privacy policies (PAPP) is measured by the following question:

- I am aware of the privacy policies of the social networking site or sites in which I participate.

Respondents who indicated that they agreed or strongly agreed with the question above are considered to have a high PAPP. Because respondents may build up a perceived awareness of the OSNs' privacy policies from channels other than the privacy policies themselves, a specific question was also included to determine whether respondents have actually read the privacy sites of the OSNs in which they participate:

- I have read the privacy policies of the social networking site or sites in which I participate.

This allows for a measurement of a general perception of respondents' awareness coupled with a measure to determine whether respondents' perception of awareness is based on whether they have actually read the privacy policies of the OSNs. It is important to note that this is a measure of *perceived* awareness, not *actual* awareness.

Based on Hypothesis 1, the majority of respondents had a high PAPP, as illustrated in Figure 12. Most of these respondents (59%) had actually read the privacy policies,

indicating that their awareness is likely based on the factual basis of privacy policies for the OSNs and not on other sources, such as hearsay. Of these respondents who had a low PAPP, almost half indicated that they had a high expectation of privacy. Conversely, amongst those respondents that had a low PAPP, the majority had a **high** EP.

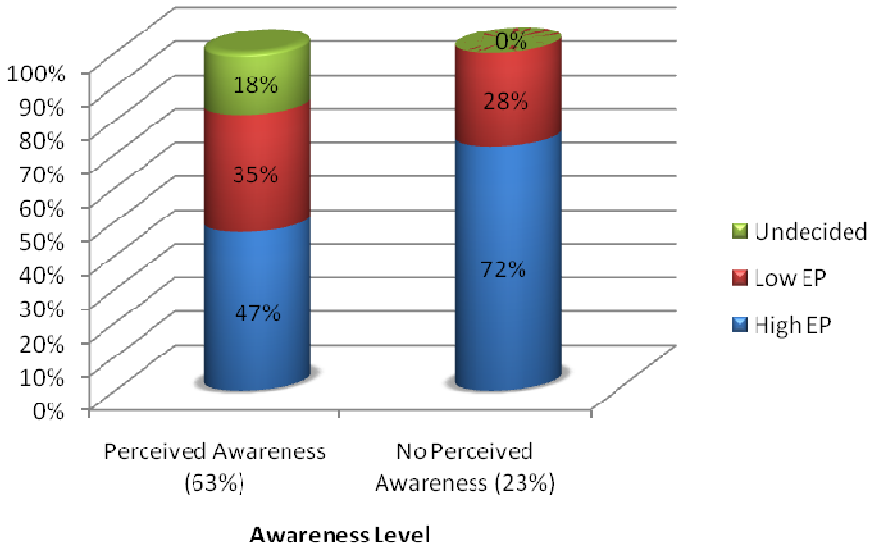

Figure 12: Contrasting the expectation of privacy between respondents with high and low perceived awareness of OSN privacy policies

Awareness does appear to influence the expectation that data posted to OSNs will remain private. Fewer respondents who had a high PAPP had a corresponding high EP than those who had a low PAPP. This may indicate that a lack of awareness builds up a false expectation of privacy. This also indicates that awareness is influenced by reading the privacy policies.

The interviewees largely confirmed these findings, with a greater awareness being found amongst those respondents who had actually read the privacy policies. It is interesting to note that most interviewees felt that other people would have a higher expectation that their data would remain private then they themselves did. This may indicate a false sense of security around interviewees' expectations of privacy.

Respondents here can be seen to be defining the boundaries across the information they consider to be personal and some evidently believe that these boundaries are supported by the privacy policies of the OSN sites. If these boundaries are not upheld, this could result in boundary turbulence (Child, et al., 2009). Metzger (2007) suggests that this boundary turbulence is often evidenced by frequent changes in privacy policies of sites, as has happened with Facebook (Opsahl, 2010), which illustrates that the implications of the privacy policies are not fully understood by many of the OSN users. An interviewee confirmed this almost verbatim by saying that their main concern was that they "don't understand the privacy settings and the implications".

As SET indicates, there is both a cost and a benefit in terms of sharing information. If an individual's expectations around the privacy of their data are *not* met, then this could cause that individual discomfort and may make them question their involvement with the OSN. One interviewee indicated that they had shut their Facebook account down as a result of privacy concerns and "people having a huge amount of friends on Facebook that can access your private information that you don't want to share and you don't want everybody seeing".

Hypothesis 2

Respondents' expectation of the privacy of their data (EDP) is measured by the following questions:

- I believe that the information posted on these sites is publicly accessible;
- I am concerned that my data will be accessed and used by third parties; and
- I believe that the data I place on social networking sites leaves a permanent trace of my actions on those sites.

These measures were developed based on the concept of the "privacy contradiction" raised by Levin & Abril (2009) and Hodge's (2006) concepts of privacy. The cautions raised by Dwyer, et al. (2007) around the permanency of OSN interactions and certain of the measures suggested by Bateman, et al. (2011) around public accessibility were also incorporated into these measures. Respondents who agreed or strongly agreed with the statements above were considered to have a **low** EDP.

Because of the different OSNs in which respondents of this survey could participate and because of differing views of the privacy policies of these OSNs, there is a potential for a mismatch should respondents simply be asked what their privacy settings are. As one interviewee confirmed, they may not always “understand the privacy settings” or “see the implications of my choices of what I choose to reveal or not”. The following question was thus also used to derive what respondents expect in relation to the privacy settings they have applied:

- I expect that the information posted on these sites will remain private to the sites themselves.

This allows respondents’ underlying expectations with regards to their privacy settings to be measured.

According to these measures, less than half of respondents (40%) were found to have a low EDP, with no respondents having a high EDP. This measure thus required a degree of weighting in order to draw conclusions from those respondents who had a varying degree of EDP. The majority of respondents who had a low EDP expected their data to remain private (58%).

On the surface, there may appear to be a conflict between respondents’ expectations that their data will remain *private* and their expectation of *privacy*. These two concepts are actually measuring different things. Respondents appear to have a high expectation of privacy but a low expectation that the data will remain private. This appears to indicate a belief amongst respondents that their data is **not** private and yet they still retain an expectation of privacy. This was confirmed by responses in the interviews where interviewees indicated that they felt the data placed on OSNs belonged to them (“it’s my data”) but that third parties, in this case banks, need to be “wise” in their use of this data and use a bit of discretion. So, although the data posted onto OSNs may be in the public domain, respondents still expect a certain amount of responsibility and caution to be applied when third parties view and consider using this data. This was further confirmed by one interviewee indicated that using OSN data in this manner is

“going very much into your private life and you as a person, not how you deal with your finances”.

As CPMT shows, although respondents have shared their data with others on OSNs, there is the perception that the data still *belongs* to the original person. There is thus the expectation that the boundaries around this data will be respected.

This appears to indicate that, in terms of Hypothesis 2, respondents largely did **not** expect their data to remain private, despite their privacy settings, although a complete conclusion cannot be drawn due to the limitation outlined above.

Hypothesis 3

In terms of Hypothesis 3, perceived control (PC) was measured by the following questions:

- I believe that I have control over the privacy of my information posted on social networking sites; and
- I believe that I have control over the use to which my information posted on social networking sites may be put.

Respondents who agreed or strongly agreed with both of these questions were considered to have a high PC over their privacy settings.

The expectation of a privacy invasion (EPI) was measured by the following questions:

- I am concerned that my data will be accessed and used by third parties.

Respondents who agreed or strongly agreed with this question were considered to have a high EPI, implied by the concern over the access and use of their data.

Only 10% of respondents had a high PC whereas 45% of respondents had a low PC. As illustrated in Figure 13, half of the respondents who had a high PC also had a high EPI. Amongst the respondents who had a low PC, the majority had a high EPI. The fact that almost half of the respondents had a low PC indicates an ongoing concern around the ability to control the privacy of one’s information online as raised by Dwyer, et al.

(2007). This is reflected by the fact that almost two-thirds of these respondents had a high EPI, indicating that respondents are concerned that their privacy will not be upheld.

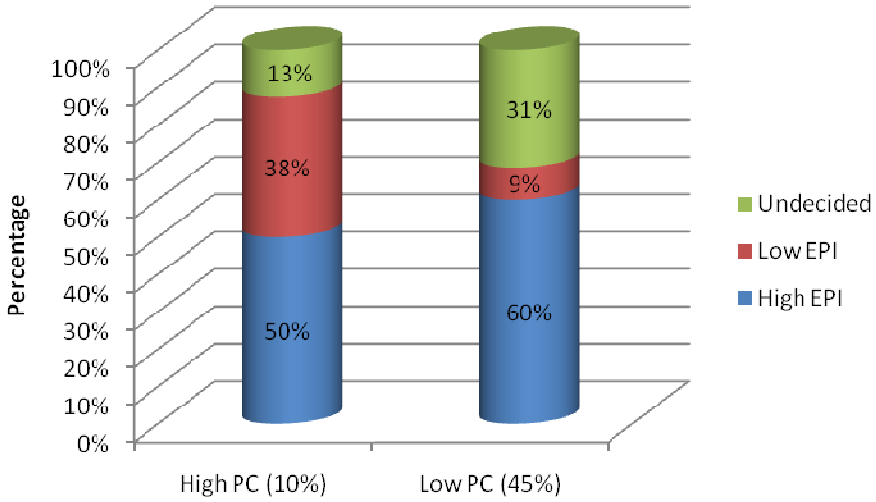

Figure 13: Contrasting the expectation of a privacy invasion between respondents with high and low perceived control over the privacy of their OSN data

One of the principles of CPMT is that, although individuals may disclose private information on OSNs, they still believe that they own that information and thus *should* be able to control access to it (Child & Petronio, 2010). In this context CPMT confirms that, for those respondents who perceive that they are unable to control the privacy of their data, there will be a greater expectation of a privacy invasion as the control over the access to their information is lacking.

Thus, in terms of Hypothesis 3, high perceived control does not appear to be related to a low expectation of a privacy invasion. On the contrary, a **low** perceived control does appear to indicate a **high** expectation of a privacy invasion. This implies that the lower the perceived control an individual has over their OSN privacy settings, the higher the expectation of a potential privacy invasion.

Hypothesis 4

Given that trust is viewed as a "three-dimensional construct" (Dimitriadis, et al., 2011), perceived trust (PT) in a respondent's primary bank is measured by the following questions:

- I believe that my primary bank looks out for my best interests (measuring benevolence);
- I believe that my primary bank is competent in the actions that they take around lending decisions (measuring competence); and
- I believe that my primary bank has integrity in the actions that they take around lending decisions (measuring integrity)

If respondents indicated that they agreed or strongly agreed with all of these questions, they are presumed to have a high PT for their primary bank.

In terms of Hypothesis 4, respondents' trust in their primary bank's use of OSN data (TSND) is measured by the question:

- I believe that the use of my data from social networking sites by banks as a basis for their lending decisions has the potential to cause me harm.

If respondents believe that the bank's use of OSN data has the potential to cause them harm, it can be extrapolated that they would not trust the bank to use their OSN data because of the underlying concern that harm could come to that customer. Thus, respondents who agree or strongly agree with the question above are considered to have a **low** TSND.

Almost half of the respondents (42%) are considered to have a high PT and only 1% of respondents are considered to have no PT in their primary bank. Edge cases where respondents only agreed or strongly agreed with only some of the measures above were not considered as the questions did not have a weighting assigned.

Amongst those respondents who have a high PT for their bank, the majority (55%) had low TSND and less than a quarter (24%) had high TSND. This indicates that the majority of respondents that trust their bank consider that their use of OSN data by the

bank has the potential to cause them harm. This was confirmed by several of the interviewees who considered that the use of their OSN data in this manner would cause those respondents to lose trust in their bank. Amongst those respondents who indicated that they trusted their bank and did not consider that the use of their OSN data by their bank could cause them harm, an interviewee indicated that this could be because they viewed the bank solely as a business and expected their bank to collect any "information that might be available in the public domain to improve their decision-making process".

In terms of Hypothesis 4, a high trust in respondents' primary banks is linked with a low trust in those banks' use of respondents' OSN data. This indicates that respondents do indeed feel that a betrayal of trust would take place should banks use respondents' OSN data to influence lending decisions. Conclusions cannot, however, be drawn around respondents who do not trust their primary bank due to a lack of data available.

In this context, SET highlights that there is a cost to the relationship between an individual and their bank with the bank's use of OSN data, which is confirmed by the negative perceptions of respondents in this regard. This cost may thus outweigh the benefits of having a relationship with this bank. This consideration around costs and benefits was highlighted by one interviewee's response where they mentioned that they "would just move banks to a bank that said they didn't unless they could show me proof somehow that what they're doing is going to benefit me in some way". As indicated previously, SET indicates that trust is a key component in building relationships so a lack of trust may cause the relationship between the customer and their primary bank to break down.

Hypothesis 5

Using the definition of betrayal from Caldwell, et al. (2009), the following measures are used to determine perceived betrayal (PB) in the context of banks' use of customers' OSN data:

- betrayal is *voluntary* and a customer can thus choose whether to feel betrayed or not. This measure is thus assumed to be satisfied by default;
- a violation of expectations *pivotal* to the nature of the relationship between the customer and their bank occurs. Banks are considered to have a fiduciary duty to their customers, which indicates that their customers will expect them to act in good faith and for their best interests (Easterbrook & Fischel, 1993). These expectations are pivotal to the nature of the relationship and this measure is thus assumed to be satisfied by default.
- both the bank and their customers are *aware* of these expectations. The following question is thus used to measure this construct:
    - I believe that my primary bank is aware of the obligations that they have toward me around the use of my social networking data;
- the expectations of the customer are violated through the *behaviour* of the bank. The following question is thus used to measure this construct:
    - I believe that my primary bank has an obligation to me not to make use of any data that I do not explicitly provide to them; and
- the customer's perception that the betrayal can *harm their wellbeing*. The following question is thus used to measure this construct as well as the construct above:
    - I believe that the use of my data from social networking sites by banks as a basis for their lending decisions has the potential to cause me harm.

Given these measures, if a respondent has agreed or strongly agreed with the questions above, it is assumed that PB has taken place. Almost a quarter (23%) of respondents thus believes that banks' use of OSN data is a betrayal of their trust. Only 3% of respondents believe that the use of OSN data is not a betrayal.

In order to determine a perceived privacy violation, the following measure was used:

- I am concerned that my data will be accessed and used by third parties

Respondents who agree or strongly agree with this question are considered to have a perceived privacy violation (PPV).

Of the group of respondents who indicated that PB could take place, a significant proportion (72%) believed that a PPV would also occur. Thus, in terms of Hypothesis 5, a perceived betrayal has a high likelihood of resulting in a perceived privacy violation. As with the measures above, the questions were not given weightings so partial scores could not be measured.

Bateman, et al. (2011) indicate that, because information is placed on OSNs via a technological interface (i.e. the Internet), there is no opportunity for personal contact with the people who are accessing and using this information. The respondents who felt that the use of OSN data is a betrayal of their trust may thus have felt that information was taken from across their boundaries without their full consent and awareness, thus causing feelings of vulnerability (Bateman, et al., 2011) and leading to the perceived betrayal and privacy violation.

Limitations and future research

The survey was targeted at colleagues and at students studying post-graduate degrees at Victoria University in Wellington. A wider audience would have allowed for greater extrapolation of the results received.

This study also did not take into account smaller banks, such as TSB, or banks solely with an online presence, such as RaboBank. Studying banks with solely an online presence may potentially give different results with regards to perceptions of trust and the use of OSN data, due to the banks' online nature.

Respondents may also have applied different privacy settings to the different OSNs in which they participate. The way in which they use the various OSNs may also differ. Twitter, for example, is seen as being a "unique social media" in that most users opt to keep their information completely public whereas users of other OSNs tend to keep their information more private (Child & Petronio, 2010). This disparity in OSN privacy settings may have caused inconsistencies in the responses to the questions around expectations of privacy and the privacy of the data.

The measures around the expectation of privacy were not weighted, meaning that there was a lack of granularity in the responses received. This prevented conclusions from being drawn for mid-range responses.

The study was unable to draw conclusions around the high expectation of data privacy as no respondents had this according to the measurements. Weighting the criteria could, again, have assisted with this.

This study has also highlighted several opportunities for future research. Future studies should aim to include customers of more New Zealand banks, including banks with an online-only presence, in order to determine the applicability of the results of this study across the New Zealand banking industry. There is also the need to differentiate the student population of the study from the non-student population to determine where differences, if any, may lie in privacy perceptions and associated expectations. Future studies should also aim to differentiate between privacy expectations across the different OSNs.

In terms of the results of this study, greater research is needed into what other factors are influencing respondents' perception of third parties' use of their OSN data. There were also gaps in this study which could be explored further around the additional factors that influence respondents' awareness of privacy policies, what respondents perceive the term "awareness" to mean in the context of privacy policies and what the actual privacy settings were in relation to respondents' expectation of data privacy and their overall expectation of privacy.

Conclusion

Respondents' expectations of privacy were influenced by their awareness of the OSN privacy policies. The less aware respondents were, the greater the expectation of privacy within OSNs. This highlights a potential for a false expectation of privacy amongst individuals who are not aware of the privacy policies of the OSN sites in which they participate. The study, however, highlighted that even respondents who did not expect their data to remain private still had an expectation of privacy. A lack of perceived control was found to be associated with a greater expectation of a privacy invasion. The majority of respondents who trusted their bank did not trust their bank's use of their OSN data. Trust in respondents' banks thus had a negative influence on those banks' use of OSN data for lending decisions.

This study has revealed a high likelihood of a perceived privacy violation taking place, should New Zealand banks follow the actions of banks in the USE with regards to the use of OSN data to influence lending decisions. It has also highlighted the need for greater care and transparency, as well as careful management of customers' expectations and trust, if New Zealand banks wish to pursue this method of influencing lending decisions. In terms of privacy on OSNs, it has also highlighted that, despite individuals' expectations, privacy is not always guaranteed. This highlights a greater need for individuals to read and understand the implications of both the privacy policies and the privacy settings of their accounts in order for them to ensure that the information that they wish to keep private does, indeed, remain so.

Appendix 1: Survey Questions

Expectation of Privacy

1. I am aware of the privacy policies of the social networking site or sites in which I participate.
2. I have read the privacy policies of the social networking site or sites in which I participate.
3. I expect that the information posted on these sites will remain private to the sites themselves.
4. I believe that the information posted on these sites is publicly accessible.
5. I am concerned that my data will be accessed and used by third parties.
6. I believe that the data I place on social networking sites leaves a permanent trace of my actions on those sites.
7. I believe that I have control over the privacy of my information posted on social networking sites.
8. I believe that I have control over the use to which my information posted on social networking sites may be put.

Trust

1. I believe that my primary bank looks out for my best interests.
2. I believe that my primary bank is competent in the actions that they take around lending decisions.
3. I believe that my primary bank has integrity in the actions that they take around lending decisions.
4. I believe that my primary bank is aware of the obligations that they have toward me around the use of my social networking data.
5. I believe that my primary bank has an obligation to me not to make use of any data that I do not explicitly provide to them.
6. I believe that the use of my data from social networking sites by banks as a basis for their lending decisions has the potential to cause me harm.

Demographic Questions

1. Are you male or female?
2. What is your age?
3. Which social networking sites do you participate in? [Selection of: Facebook, MySpace, LinkedIn, Other]

4. Which is your primary bank? [Choice of: The National Bank, ANZ, Westpac, ASB, Kiwibank, TSB]
5. Would you be prepared to take part in a follow-up interview based on the results of this interview? [Yes/No]
6. Would you be interested in receiving a copy of this research once it has been completed? [Yes/No]

Appendix 2: Interview Questions

Privacy

1. What are your expectations around the privacy of the information that you place on social networking sites?
2. What are your concerns around the privacy of the information that you place on social networking sites?
3. What are your opinions on the fairness of banks using data from social networking sites to influence their lending decisions?

Trust

1. What are your perceptions of your primary bank as a benevolent entity?
2. What are your expectations around banks' use of your data from social networking sites?
3. How does your trust of your primary bank influence the fact that they may use your publicly accessible data from social networking sites to influence their lending decisions?

General

1. If you have any other comments to make, please state them now.

Appendix 3: Question Data[1]

Q1. I am aware of the privacy policies of the social networking site or sites in which I participate.				
Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
10	56	15	18	1

Q2. I have read the privacy policies of the social networking site or sites in which I participate.	
Yes	No
42	58

Q3. I expect that the information posted on these sites will remain private to the sites themselves.				
Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
21	27	16	29	7

Q4. I believe that the information posted on these sites is publicly accessible				
Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
19	45	15	18	3

Q5. I am concerned that my data will be accessed and used by third parties.				
Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
19	41	26	10	3

Q6. I believe that the data I place on social networking sites leaves a permanent trace of my actions on those sites.				
Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
40	53	6	2	0

Q7. I believe that I have control over the privacy of my information posted on social networking sites.				
Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
2	31	20	37	10

[1] Data provided as a percentage

Q8. I believe that I have control over the use to which my information posted on social networking sites may be put.				
Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
2	15	22	47	15

Q9. I believe that my primary bank looks out for my best interests.				
Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
8	41	24	21	6

Q10. I believe that my primary bank is competent in the actions that they take around lending decisions.				
Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
12	62	20	7	0

Q11. I believe that my primary bank has integrity in the actions that they take around lending decisions.				
Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
11	60	23	6	0

Q12. I believe that my primary bank is aware of the obligations that they have toward me around the use of my social networking data.				
Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
7	37	41	14	1

Q13. I believe that my primary bank has an obligation to me not to make use of any data that I do not explicitly provide to them.				
Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
34	31	11	22	2

Q14. I believe that the use of my data from social networking sites by banks as a basis for their lending decisions has the potential to cause me harm.				
Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
15	40	20	21	3

Q15. Are you male or female?	
Male	Female
57	43

Q16. What is your age?[2]				
21-30	31-40	41-50	51-60	61+
30	43	21	5	1

Q17. Which social networking sites do you participate in?			
Facebook	MySpace	LinkedIn	Other
92	7	52	19

Q18. Which is your primary bank?						
ANZ	ASB	BNZ	KiwiBank	The National Bank	TSB	Westpac
11	23	15	11	29	0	11

Q19. Would you be prepared to take part in a follow-up interview based on the results of this interview?	
Yes	No
43	57

Q20. Would you be interested in receiving a copy of this research once it has been completed?	
Yes	No
56	44

[2] This field was a numeric, free-text entry. The age bands of data have been provided.

References

ASB Bank Limited. (2009). Privacy - ASB Bank New Zealand. Retrieved 22 July, 2011, from https://www.asb.co.nz/story335.aspx

ASB Bank Limited. (2011). ASB Careers 4u. Retrieved 21 July, 2011, from https://careers.asbgroup.co.nz/asb/our-people

Awad, N. F., & Krishnan, M. S. (2006). The Personalisation Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalisation. *MIS Quarterly, 30*(1), 13-28.

Baird, C. H., & Gonzalez-Wertz, C. (2011). How top performers achieve customer-focused market leadership. *Strategy & Leadership, 39*(1), 16-23.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. First Monday, *11*(9).

Bateman, P. J., Pike, J. C., & Butler, B. S. (2011). To disclose or not: publicness in social networking sites. *Information Technology & People, 24*(1), 78-100.

Berman, J., & Bruening, P. (2001). Is Privacy Still Possible in the Twenty-first Century? *Social Research, Spring 2001*, 306-318.

Bloland, H. G. (1989). Higher Education and High Anxiety: Objectivism, Relativism, and Irony. *The Journal of Higher Education, 60*(5), 519-543.

Boot, A. W. A., & Marinĉ, M. (2008). The evolving landscape of banking. *Industrial and Corporate Change, 17*(6), 1173-1203.

Brandenburg, C. (2008). The Newest Way to Screen Job Applicants: A Social Networker's Nightmare. *Federal Communications Law Journal, 60*(3), 597-626.

Butterworth, S. (2008). The readers' editor on ... the mining of social networking sites for information. Retrieved 21 July, 2011, from

http://www.guardian.co.uk/commentisfree/2008/jan/07/leadersandreply.mainsection

Caldwell, C., Davis, B., & Devine, J. A. (2009). Trust, Faith and Betrayal: Insights from Management for the Wise Believer. *Journal of Business Ethics, 84*, 103-114.

Cazier, J. A., Shao, B. B. M., & St. Louis, R. D. (2006). E-business differentiation through value-based trust. *Information & Management, 43*(6), 718-727.

Chen, J., Ping, W., Xu, Y., & Tan, B. C. Y. (2009). *Am I Afraid of My Peers? Understanding the Antecedents of Information Privacy Concerns in the Online Social Context.* Paper presented at the Thirtieth International Conference on Information Systems, Phoenix.

Child, J. T., Pearson, J. C., & Petronio, S. (2009). Blogging, Communication, and Privacy Management: Development of the Blogging Privacy Management Measure. *Journal of the American Society for Information Science and Technology, 60*(10), 2079-2094.

Child, J. T., & Petronio, S. (2010). *Unpacking the paradoxes of privacy in CMC relationships: The challenges of blogging and relational communication on the internet*. Cresskill, NJ: Hampton Press.

Clark, L. A., & Roberts, S. J. (2010). Employer's Use of Social Networking Sites: A Socially Irresponsible Practice. *Journal of Business Ethics, 95*, 507-525.

comScore. (2010). Russia Has Most Engaged Social Networking Audience Worldwide. Retrieved 21 October, 2011, from http://www.comscore.com/Press_Events/Press_Releases/2010/10/Russia_Has_Most_Engaged_Social_Networking_Audience_Worldwide

comScore. (2011a). Facebook Users in Argentina Spend 9 Hours a Month on Site, Second Only to Israel in User Engagement. Retrieved 21 October, 2011, from http://www.comscore.com/Press_Events/Press_Releases/2011/6/Facebook_Users_in_Argentina_Spend_9_Hours_a_Month_on_Site

comScore. (2011b). In New Zealand, Females Spend Significantly More Time Social Networking than Males. Retrieved 21 October, 2011, from http://www.comscore.com/Press_Events/Press_Releases/2011/7/In_New_Zealand_Females_Spend_Significantly_More_Time_Social_Networking_than_Males

Cropanzano, R., & Mitchell, M. S. (2005). Social Exchange Theory: An Interdisciplinary Review. *Journal of Management, 31*(6), 874-900.

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication, 15*(83-108).

Dimitriadis, S., Kouremenos, A., & Kyrezis, N. (2011). Trust-based segmentation: Preliminary evidence from technology-enabled bank channels. *International Journal of Bank Marketing, 29*(1), 5-31.

Dwyer, C., Hiltz, S., & Passerini, K. (2007). *Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace.* Paper presented at the Thirteenth Americas Conference on Information Systems, Keystone, Colorado.

Easterbrook, F. H., & Fischel, D. R. (1993). Contract and Fiduciary Duty. Journal of Law and Economics, 36(1), 425-446.

Edwards, R. M., & Kleiner, B. H. (2002). Conducting Effective and Legally Safe Background and Reference Checks. *Managerial Law, 44*(1/2), 136-150.

Emerson, R. M. (1976). Social Exchange Theory. Annual Review of Sociology, 2, 335-362.

Facebook. (2011). Data Use Policy | Facebook. Retrieved 29 October, 2011, from http://www.facebook.com/about/privacy/your-info-on-fb

Festinger, L. (1957). *A theory of cognitive dissonance*. United States of America: Stanford University Press.

Finney, M. (2010). Banks mining social media sites for personal info. Retrieved 24 April, 2011, from http://abclocal.go.com/kgo/story?section=news/7_on_your_side&id=7283384

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behaviour, 25*, 153-160.

Gerzema, J., & D'Antonio, M. (2011). The Power of the Post-Recession Consumer. *strategy+business, Spring 2011*.

Hodge, M. J. (2006). The Fourth Amendment and Privacy Issues on the "New" Internet: Facebook.com and MySpace.com. *Southern Illinois University Law Journal, 31*, 95-123.

KiwiBank. (2011a). Awards - Kiwibank. Retrieved 06 November, 2011, from http://www.kiwibank.co.nz/about-us/more-about-us/awards.asp

KiwiBank. (2011b). Code of banking responsibility - Kiwibank. Retrieved 21 July, 2011, from http://www.kiwibank.co.nz/about-us/more-about-us/code-of-banking-responsibility.asp

KiwiBank. (2011c). Privacy and Security - Kiwibank. Retrieved 22 July, 2011, from http://www.kiwibank.co.nz/privacy-and-security/

Lenhart, A. (2009). *The Democratization of Online Social Networks: A Look at the Change in Demographics of Social Network Users over Time*. Milwaukee, WI: Pew Research Center Internet & American Life Project.

Levin, A., & Abril, P. S. (2009). Two Notions of Privacy Online. *Vanderbilt Journal of Entertainment and Technology Law, 11*(4), 1001-1051.

Luo, X. (2002). Trust Production and Privacy Concerns on the Internet: A Framework Based on Relationship Marketing and Social Exchange Theory. *Industrial Marketing Management, 31*(2), 111-118.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709-734.

Meredith, P. (2006). Facebook and the Politics of Privacy. Retrieved 21 July, 2011, from http://motherjones.com/politics/2006/09/facebook-and-politics-privacy

Metzger, M. J. (2007). Communication Privacy Management in Electronic Commerce. *Journal of Computer-Mediated Communication, 12*(2), 1-27.

Morgan, R. M., & Hunt, S. D. (1994). The Commitment-Trust Theory of Relationship Marketing. *Journal of Marketing, 58*(3), 20-38.

Nissenbaum, H. (1998). Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy, 17*(5/6), 559-596.

O'Neill, R. (2011). We reveal the country's best banks. Retrieved 06 November, 2011, from http://www.stuff.co.nz/sunday-star-times/business/5516141/We-reveal-the-countrys-best-banks

Onwuegbuzie, A. J., Johnson, R. B., & Collins, K. M. T. (2009). Call for mixed analysis: A philosophical framework for combining qualitative and quantitative approaches. *International Journal of Multiple Research Approaches, 3*, 114–139.

Opsahl, K. (2010). Facebook's Eroding Privacy Policy: A Timeline. Retrieved 1 November, 2011, from https://www.eff.org/deeplinks/2010/04/facebook-timeline

Petronio, S. (2007). Translational Research Endeavors and the Practices of Communication Privacy Management. *Journal of Applied Communication Management, 35*(3), 218-222.

Pike, J. C., Bateman, P. J., & Butler, B. S. (2009). *I Didn't Know You Could See That: The Effect of Social Networking Environment Characteristics on Publicness and Self-Disclosure.* Paper presented at the Fifteenth Americas Conference on Information Systems, San Francisco, California.

Privacy Commissioner. Purpose for collection of personal information (principle one). Retrieved 14 July, 2011, from http://privacy.org.nz/purpose-for-collection-of-personal-information-principle-one

Punch, K. F. (2005). *Introduction to Social Research: Quantitative and Qualitative Approaches* (Second ed.). London: SAGE Publications Ltd.

RaboDirect. (2011). Public confidence in finance sector drops while people say investments worth more. Retrieved 25 April, 2011, from http://www.rabodirect.co.nz/rabodirect-tv-radio-ads/2011/financial-confidence-index-press-release-new-zealand-april-2011.aspx

Reynolds, G. W. (2010). *Ethics in Information Technology* (Third ed.). United States of America: Course Technology, Cengage Learning.

Richardson, G. (2001). Social Exchange Theory - Interpersonal Communication Context. Retrieved 17 October, 2011, from http://www.uky.edu/~drlane/capstone/interpersonal/socexch.html

Ryder, M. (2008). The Cyborg and the Noble Savage: Ethics in the war on information poverty. Retrieved 28 March, 2010, from http://carbon.ucdenver.edu/~mryder/savage.html#def_constructivism

Schmeck, R. (1997). Content Analysis. Retrieved 18 April, 2010, from http://mccoy.lib.siu.edu/projects/psyc/schmeck/iv2.ppt

Schonlau, M., van Soest, A., Kapteyn, A., & Couper, M. (2009). Selection Bias in Web Surveys and the Use of Propensity Scores. *Sociological Methods & Research, 37*, 291-318.

Slevin, J. (2000). *Publicness and the Internet. The Internet and Society*. Cambridge: Polity Press.

Srinivasan, R., Lilien, G. L., & Rangaswamy, A. (2002). Technological opportunism and radical technology adoption: An application to e-business. *Journal of Marketing, 66*(3), 47-60.

Steeves, V. (2008). If the Supreme Court Were on Facebook: Evaluating the Reasonable Expectation of Privacy Test from a Social Perspective. *Canadian Journal of Criminology and Criminal Justice, 50*(3), 331-347.

Talja, S., Tuominen, K., & Savolainen, R. (2005). "Isms" in information science: constructivism, collectivism and constructionism. *Journal of Documentation, 61*(1), 79-101.

The National Bank of New Zealand. (2011a). National Bank - Commitments. Retrieved 21 July, 2011, from http://www.nbnz.co.nz/promos/customercommitments/

The National Bank of New Zealand. (2011b). Privacy Policy. Retrieved 22 July, 2011, from http://www.nbnz.co.nz/terms/privacy.aspx

The New York Times. (2011). Facebook, Inc. News. Retrieved 10 October, 2011, from http://topics.nytimes.com/top/news/business/companies/facebook_inc/index.html

The Telegraph. (2011). Facebook users 'can't keep up with privacy changes'. Retrieved 06 November, 2011, from http://www.telegraph.co.uk/technology/facebook/8868065/Facebook-users-cant-keep-up-with-privacy-changes.html

Timm, D. M., & Duven, C. J. (2008). *Using emerging technologies to enhance student engagement: New directions for student services*. San Francisco, CA.: Jossey-Bass.

TSB Bank Limited. (2009). TSB Bank - Privacy Statement. Retrieved 22 July, 2011, from http://www.tsb.co.nz/Info/PrivacyStatement.aspx

Valenzuela, D., & Shrivastava, P. (2002). Interview as a Method for Qualitative Research. Retrieved 18 April, 2010, from http://www.public.asu.edu/~kroel/www500/Interview%20Fri.pdf

Wagner, T., Lutz, R. J., & Weitz, B. A. (2009). Corporate hypocrisy: overcoming the threat of inconsistent corporate social responsibility perceptions. *Journal of Marketing, 73*, 77-91.

Ware, W. H. (1984). Information systems security and privacy. *Communications of the ACM, 27*, 315-321.

Westin, A. F. (1967). *Privacy and Freedom*. Athenaeum, New York.

Westpac New Zealand Limited. (2008). Westpac New Zealand Working for Westpac. Retrieved 21 July, 2011, from http://www.westpac.co.nz/olcontent/olcontent.nsf/Content/Working+for+Westpac

Worthington, S., & Welch, P. (2011). Banking without the banks. International Journal of Bank Marketing, 29(2), 190-201.