The Value Congruence of Social Networking Services - a New Zealand Assessment of Ethical Information Handling

Tony Hooper and Tyrone Bard Evans
Victoria University of Wellington, New Zealand
tony.hooper@vuw.ac.nz
evanstyro@myvuw.ac.nz

Abstract: Social networking sites on the Internet have enjoyed considerable media publicity recently. Whereas conventional social interactions leave behind no record, similar social interactions performed on social networking websites, can leave behind detailed and possibly permanent records. A literature review of social networking sites and personal privacy indicates that users may be unwary when interacting with specific social networking sites and unaware of the potential consequences of interaction, or they may deliberately ignore the risks in preference for publicity and personal relationships. A content analysis was carried out to compare the "terms of use" and privacy statements of six social networking sites with one another. The twelve principles of the New Zealand Privacy Act of 1993 were used in the coding template because they represent the agreed national values on information handling in New Zealand. The study demonstrated significant shortcomings in the contractual relationships between the users and social networking services that could be exploited in order to misuse personally identifiable data. It highlighted the need for users and organisations to be aware of the terms of use and privacy statements to which they become contractually bound, as well as to understand what the network may do with user's information. Particular concern related to the accuracy of the information collected and the deletion of historic data. Social networking services terms of use and privacy statements appear to be more concerned with exculpatory clauses than demonstrating a concern for user security. Because many users, especially adolescents, are more driven by peer group pressure and the behavioural conventions of their age cohort than concern for the dangers they face when posting personal information, current theory on the role of trust in online transactions is failing to explain the contemporary behavioural phenomenon of SNS use. The social responsibility implications arising from this phenomenon and the accountability of SNSs for any misuse of personally identifiable information through their websites are discussed. Some areas for further research are suggested.

Keywords: social networking services, value congruence, New Zealand Privacy Act 1993, privacy policies, personal security, personally identifiable information

1. Introduction

In New Zealand, the principles of the Privacy Act (1993) define the agreed national values and privacy rights of citizens and, by extension, of online customers. These principles can therefore be used as a basis on which business websites can be evaluated for conformity to agreed national values. A website privacy notice is a form of contractual commitment on the part of the company receiving the information, and one of the primary means customers have to identify the values of an organisation. It has been shown that customers are more likely to transact with businesses that share their values (Cazier, 2006; Meinert et al, 2006). The purpose of the study was to examine the extent to which Social Network Services (SNS) websites conform to the national values on the rights of individuals to information privacy. Accordingly, this research analyses the "terms of use" and privacy statements of six social networking sites - Twitter, Facebook, Bebo, Habbo, LinkedIn, and Myspace against the agreed national values on information handling promulgated in the New Zealand Privacy Act of 1993. The paper argues for the use of privacy legislation as a framework for evaluating online information handling practices and makes some recommendations on ways that SNSs can improve their value congruence and demonstrate their business integrity. National values on information handling as identified in privacy legislation need to be publicised and promoted in order to alert citizens to the criteria by which they might assess their vulnerability to exploitation in the virtual social environment. Because many users, especially adolescents, are more driven by peer group pressure and the behavioural conventions of their age cohort than concern for the dangers they face when posting personal information, current theory is failing to explain the contemporary behavioural phenomenon of SNS use.

Reference this paper as:
Hooper, T and Evans, T, B. "The Value Congruence of Social Networking Services - a New Zealand Assessment of Ethical Information Handling" *The Electronic Journal Information Systems Evaluation Volume 13 Issue 2 2010, (pp121 - 132), available online at www.ejise.com*

2. Literature review

2.1 Social networking services and the nature of the problem

Social Network Services (SNS) are web applications that facilitate online relationships between people. They allow users to communicate, form and maintain relationships by providing a means to remain in contact with friends, family, colleagues and associates (Haythornthwaite, 2005). SNSs require users to contribute personal information in order to interact with other users, but have no moral securities imbedded (Weiss, 2009). Cazier, Wilson & Medlin (2002) noted that the technological basis for Social Network Services is designed to promote the unrestricted sharing of information while remaining morally neutral. The result is a user profile that may include information such as date of birth, age, relationships status, likes, dislikes, interests, religion, ethnicity and photographs (Boyd & Ellison, 2007; Dwyer, Hiltz & Passerini, 2007). While the information is provided by the user of the service in order to facilitate communication with other users, the moral neutrality of the technology may not apply to the business model, Posted information may be used for other purposes that are not always made clear by the SNS. Social networking sites are for-profit and their revenue models focus on the use of advertising to their millions of users. However being motivated by profit can overshadow concerns for user privacy (Fernandez, 2009). SNS privacy issues have arisen from the personal information willingly disclosed in personal profiles. From this information it is possible to reconstruct social security numbers or other personal identifiers that can be used for fraudulent activity. Because the information is voluntarily made public, it can be argued that such privacy infringement is the result of poor user awareness and education rather than the responsibility of the SNS (Weiss, 2009).

Access to much personal information available on SNS websites is of importance to marketing and advertising personnel. Personal information obtained using the Internet is easier to assemble than traditional means of data collection, but can have an undesirable side effect for the user (Preibusch et al., 2007). Business and other organizations are discovering the capabilities SNSs can offer by way of networking opportunities and improving employee relationships (Haythornthwaite, 2005). Governments and law enforcement agencies have also taken an interest in SNS information vulnerability with regard to terrorism, criminals and illegal or immoral activity (Preibusch et al., 2007). As a result, the reputation of social networking sites has been diminished by a number of incidents publicized by the news media (Chiaramonte and Martinez, 2006). Social networking sites usually record all interactions, and retain them for potential future use. The press has emphasized privacy concerns, especially concerning younger users (Kornblum & Marklein, 2006). In an academic study of privacy and social networking sites, Gross and Acquisti (2005) analyzed 4,000 university student Facebook profiles and detailed the potential privacy threats resulting from the personal information students had included on the site. Potential threats included the ability to reconstruct students' social security numbers using information often found in profiles, such as hometown and date of birth, and to use this to open accounts, and gain access to other information. Hodge (2006) argued that the U.S. Constitution and legal decisions concerning privacy are not equipped to address social network sites. He raised the question whether police officers have the right to access content posted on Facebook without a warrant. The issue hinges on users' expectations of privacy and whether or not SNS profiles are considered public or private. Privacy becomes a major concern when personal information is used for purposes other than intended or when it is fraudulently re-used (Preibusch et al., 2007).

2.2 Privacy on the internet

The Internet has become a primary and global medium for the gathering of personal information. Internet activity generates information about a user for advertisement targeting (Kolbitsch & Maurer, 2006). The Internet allows for the easy and cheap collection of large amounts of information, frequently without the knowledge or consent of the online customer (Slane, 2001; Stahl, 2004). Often a website collects data on the first contact with it, before a user is aware or can view the privacy notice (Pollach, 2005). Even if a customer is only visiting a website, the computer is at least partially identifiable through its IP address. After the organisation has the information, renegotiation is difficult and consumers have very little power to stop the organisation from using it or sharing it with others.

The paucity of privacy polices on websites, campaigning by dissatisfied users and media coverage of information violations and invasions (Bialek & Smedresman 2008; Kruck, Gottovi, Moghadami, Broom & Forcht, 2002) have all contributed to the concern. It has also been found that privacy policies are often confusing, incomplete or inconsistent (Luo, 2002). Statements protecting personal information to the extent of the law, when the law protects so little, allows for deliberate misuse of data without the

need for consent. Additionally, the global connectivity of the Internet also complicates privacy protection due to the variation of information handling laws in different jurisdictions (Kruck et al., 2002). Personal privacy violations are often caused by human unawareness. Fernandez (2009) investigated information privacy and found that the level of security users put on their profile does not mean that they retain full control over how their information is used on social networking websites. The "terms of use" and privacy statements can be used to hide actual business intentions or to protect the online business against prosecution (Preibusch et al., 2007). Several tactics have been used to relieve users of their privacy concerns in order to collect their personal information. One report (Rauhofer, 2009) put forward the notion that privacy was a tradable object under the control of the rights holder. The risk of information privacy loss was weighed against personal security, loss of material gain and loss of convenience. It would appear easier therefore to justify privacy intrusions if the benefit is significant. National or personal security concern is used in politics frequently to this end. Zorn (2006) maintains that total online privacy simply isn't possible.

2.3 Value congruence

While the notion of trust in electronic commerce and internet business has been the focus of researchers for several years, the issue with SNSs is not entirely related to trust. Both Wang & Emurian (2005) and Hoofnagle & King (2008) demonstrated that internet users are prepared to accept a certain amount of risk, based on positive expectations of a site's intentions. Oermann & Dittmann (2006) found that people are willing to bestow their trust if the expected advantage is greater than the possible disadvantage. Barnes (2006, p11.) found that the real issue was "the social behaviour of teenagers on the Internet and the use and misuse of their private information". She argued that "social networking companies and advertisers need to establish policies about the proper use of personal information posted on these sites" (Barnes, 2006, p10). The question arises "what are the values of our society that would inform us of the 'proper use of personal information'?" Recent research by Cazier (2006) has determined that users are more comfortable and confident using a website if the site – and thus the organisation – has values in common with their own. Cazier (2006) defined "value congruence" as the degree of overlap between potential customers' values and the values they perceive an organisation possesses. Higher levels of value congruence between employees and the organization equates to greater levels of support, commitment and satisfaction towards organisational objectives (Cazier et al., 2007; Edwards & Cable, 2009). Newman and Nollen (1996) found empirical evidence that high business performance by multinational enterprises resulted from the adaptation of their management practises to the national culture in which they operate.

2.4 Determining national values on information handling

In New Zealand, national values on information handling find expression in the provisions of the Privacy Act (1993). This Act provides for "how personal information can be collected, used, stored and disclosed", rather than legislating a right to privacy (NZ Privacy Commissioner, n.d.). It identifies twelve principles of privacy (see Table One below), following the OECD convention of 1981. The twelve privacy principles attempt to balance the interests of business with consumer privacy concerns, based on good business practice. They are written in a technology neutral way so that they can apply to both the online and "bricks and mortar" worlds (Slane, 2001). The Act recognises the importance of business taking some responsibility for privacy protection, (Slane, n.d.) pointing out that the costs of privacy compliance would have to be borne in any case in the age of consumer privacy awareness.

Table 1: Summary of privacy principles of the New Zealand Privacy Act, 1993

Principle 1	Purpose of collection	Information must be collected for a lawful purpose connected with the function of the collecting agency and be necessary for that purpose.
Principle 2	Source of information	Personal information must be collected directly from the individual concerned, with certain exceptions.
Principle 3	Collection of information from subject	A collecting agency must ensure an individual knows of the collection and its purpose, intended recipients, name and address of collecting and holding agencies, and consequences of withholding information.
Principle 4	Manner of collection	Information must not be collected by means that are unlawful, unfair or intrusive.
Principle 5	Storage and	Information must be stored securely against loss, access, use,

	security	modification or disclosure, except with holding agency authority.
Principle 6	Access to information	An individual is entitled to confirm that personal information is held by an agency and have access to the information.
Principle 7	Correction of information	An individual is entitled to request the correction of personal information.
Principle 8	Accuracy of information	Before use, an agency must ensure information is accurate, up to date, complete, relevant and not misleading.
Principle 9	Limits on holding information	An agency must not hold personal information longer than required for the lawful purposes of use.
Principle 10	Limits on use of information	Information must not be used for any other purpose than that for which it was collected, with certain exceptions.
Principle 11	Limits on disclosure of information	Information must not be disclosed unless the agency believes the disclosure is directly related to the purposes for which it was collected, with certain exceptions.
Principle 12	Unique identifiers	An agency must not assign a unique identifier to an individual unless it is necessary for carrying out agency functions.

Because the principles of information control articulated in privacy protection legislation have been carefully considered beforehand, tested in parliament and other consultative fora, and then enshrined in legislation, those principles can be considered to reflect the values of the people in that national jurisdiction. It would be hard to imagine a better or more thorough mechanism for achieving consensus on such a wide-ranging and complex issue. Furthermore, the application of the Act, through the published deliberations of the Privacy Commissioner, maintains the currency of those values. Accordingly, one may assume that the Privacy Act articulates the national values on the rights of individuals to control information about themselves. The principles of the Act can provide the criteria against which Internet websites can be assessed for conformity to national values. The extent to which businesses demonstrate congruent values through their website privacy notices becomes an important indicator of value congruence. The same applies to SNSs.

3. Methodology

In the social sciences, ontologies are used to understand the nature of social reality (Blaikie, 2007, p. 13). In this case, the research assumes an idealist position that what is being observed has no independent existence apart from the perceptions of the observer. The post-positive epistemology is based on the belief that to understand the social world one needs to understand the points of view of those being studied. The philosophical paradigm for this research aligns with the interpretive tradition, seeking to understand the "deeper structure of a phenomenon" to obtain a shared understanding of the phenomenon (Orlikowski & Baroudi, 1991, p. 5). This paradigm focuses on exploring meaning in context in order to develop an in-depth understanding of the context of the phenomenon (Myers, 2009, p.39). One of the benefits of interpretive research is that it allows the researchers to interpret what they see and understand (Orlikowski & Baroudi, 1991, p 15). Consequently, these interpretations cannot be separated from the background, history, contexts and prior understandings of the researchers themselves (Creswell, 2009, p. 176). Content analysis is a "research technique for making replicable and valid inferences from data to their context" (Krippendorf, 1980). It has also been defined as a research technique to isolate and assess aspects of communications (Ecole Polytechnique, 2001). Holsti (1968, p. 608) defined it as "any technique for making inferences by systematically and objectively identifying special characteristics of messages." According to Bruce and Berg (2001) content analysis can be applied to "manifest content" (ie those elements that are physically present and countable), as well as to "latent content" (ie. an interpretative reading of the symbolism underlying the physical data).

A website symbolically represents the owning institution and contains material indicating its business purpose and intentions. A content analysis of the website's "terms of use" and privacy statements is considered a valid means for examining the values of that organisation. This study analysed the websites of six SNSs using the 12 provisions of the New Zealand Privacy Act of 1993 in the sampling frame as the basis for comparison. These statements were accessed from the social networking services homepages at the following URLs:-

- Facebook (www.facebook.com)

- Bebo (www.bebo.com)
- Twitter (www.twitter.com)
- Habbo (www.habbo.com)
- LinkedIn (www.linkedin.com)
- MySpace (www.myspace.com)

Data validation was ensured by using fourteen independent research assistants to analyse the websites using the same frame. The analyses were compared and where the data was in agreement it was accepted. Contradictory entries were then investigated by the primary researcher to establish a final data entry. Tabulation of the coding template analysis can be found in Appendix 1.

4. Analysis of SNS privacy and" Terms of Use" statements

The small sample size of six SNS websites, and the fact that only the principles of the New Zealand Privacy Act were used means that, at best, the results can only be indicative. The analysis of the websites indicated that none of the SNSs met all the requirements set out in the 12 Privacy Principles. A more detailed analysis and discussion follows.

Principle 1 – Information must be collected for a lawful purpose connected with the function of the collecting agency and be necessary for that purpose. Clearly, there is nothing unlawful about sharing information with friends or determining who may see one's personal information. All SNSs gather their information directly from the users as an integral part of their service. By using the site, visitors, members or customers agree to be bound by and indicate acceptance of and compliance with the terms of use and the privacy principles of the SNS concerned. Individuals are warned that by accessing the site, personally identifiable information may be gathered and processed, and that they alone are responsible for any content posted and the consequences that might flow from posting that data. As a result, SNSs can argue that they have warned their users, visitors or customers of the dangers, and that they therefore have no further obligations. The hidden, uncertain element here relates to the use that is made by the SNS of the information posted or that is garnered from click analysis and cookies.

Principle 2 – Personal information must be collected directly from the individual concerned – unless the information is publicly available. All SNSs specify that all information or content is the sole responsibility of the person contributing it. However, without attempting to identify the customer through tracking the IP address, receipt of email or other means, SNSs are unable to guarantee that the information they receive comes from the individual concerned. Besides data contributed by users and customers, the method of collection is specified as being cookies, web-beacons, and other technologies "to recognize you, customize your experience and serve advertisements" (LinkedIn Privacy Policy). Some SNSs recognise that "third parties" may post information to the site, or misuse personal information, and that they have no control over that use. Facebook admits that it may also use information about users "that we collect from other sources" such as newspapers, blogs and other users of Facebook. Users are "generally" allowed to opt out, or to limit the connection of such information to their profile.

Principle 3 – A collecting agency must ensure an individual knows of the collection and its purpose, intended recipients, name and address of collecting and holding agencies, and consequences of withholding information. SNSs do not provide names and addresses of the collecting and holding agencies. What is done with the information is not always specified, except in vague terms such as making the information available to "trusted third parties", or "to improve and customize" services to users. Clearly, personal information provided by users will be made available to other people who are not excluded by the privacy constraints determined by the users themselves. And users have the right to access the personal information others wish to share with them according to their own privacy settings. The problems arise with "trusted third parties" and "affiliated companies and organizations" that are not necessarily specified. They may be trusted by the SNS, but not necessarily by the users whose information is being distributed. After contributing their personal information users lose control over what is done with it and over any possible consequences for themselves.

Principle 4 – Information must not be collected by means that are unlawful, unfair or intrusive. If the information is being provided voluntarily by adults, who are assumed to have read the "terms of

use" and privacy statements, then it would be hard to argue that collection was unfair, unlawful or intrusive. However, one could question the corporate social responsibility of the SNS towards the providers of the information that form the basis of the services offered.

Principle 5 – Information must be stored securely against loss, access, use, modification or disclosure, except with holding agency authority.

Many providers offer their users industry standard levels of security and storage technology. LinkedIn offers SSL encryption for all password protected and sensitive data. Facebook also noted that their servers were secured behind a firewall and Bebo stated that they comply with the EU standards for data protection. MySpace and Twitter both acknowledge that they take administrative, technical and physical measures but both providers fail to give any details. Some (Facebook, BEBO, LinkedIn) are licensees of the TRUSTe Privacy Program that has been established to promote fair information practices on the Internet. However, by its very nature shared personal information cannot be entirely secure and there is justifiable concern about how such information can be misused.

Principle 6 – An individual is entitled to confirm that personal information is held by an agency and to have access to the information. Having contributed their personal information or communications users of SNSs are assumed to know exactly what information is held. They can access some if not all of that information. What is not always accessible, or even known, are the interactions or postings that have been archived. Users also do not know what use has been made of their postings by "friends" or "friends of friends".

Principle 7 – An individual is entitled to request the correction of personal information. While SNSs acknowledge that users may change their information, none offer confirmation that correction or deletion of archived files have been made or that agencies to which information has been disclosed will also be informed, and the information corrected. Rather, the SNSs ensure that their "terms of use" and privacy statements devolve responsibility entirely on the users. Twitters policy enables the user to modify their data, but this process is done by the Twitter staff through an email system. No confirmation of correction or change is offered.

Principle 8 – Before use, an agency must ensure information is accurate, up to date, complete, relevant and not misleading. The responsibility for keeping information up to date lies with the customer, member or user, as specified in the terms of use statements. However the legal requirement is for the SNSs to ensure that all personal information collect directly by them is accurate. Bebo, Facebook and Habbo all included a clause in their Terms of Use that stated all information provided must be accurate and not misleading. However it did not indicate that data would be checked. MySpace was the only provider that stated it would take reasonable steps to check information provided for accuracy but in reality there is no way to know for sure. LinkedIn provided no reference at all. The site being for professionals, presumably it was felt this provision was not necessary.

Principle 9 – An agency must not hold personal information longer than required for the lawful purposes of use. The chillingly permanent allocation of an "unconditional, unlimited, worldwide, irrevocable, perpetual" licence to Habbo and something similar to LinkedIn seems to indicate that SNSs do not have an efficient and considered retention and disposal program. Nor do they articulate their intention of disposing of users' information in a way that accords with this principle. The problem arises when users leave the SNS and do not know whether their information has been entirely deleted, or if it has been sent on to some "trusted third party" and can no longer be accessed, corrected or deleted.

LinkedIn was alone in specifically stating that information would be wiped from their system after account deletion. MySpace and Facebook included these sections, but they were weak or conditional. MySpace stated that personal information could be deleted from their system by request. Facebook mentioned that on account deletion, information may persist in backup for a short period. However this only hints at deletion and does not state it specifically. Bebo, Habbo and Twitter however made no mention of deletion in their statements.

Principle 10 – Information must not be used for any other purpose than that for which it was collected, with certain exceptions. The exceptions to this principle are where information is publicly

available, or the use is authorized, or that non-compliance is necessary for legal or public protection reasons. SNSs notify customers through their "terms of use" and privacy statements that their personal information is used for several purposes or "made available" (sold?) to third parties. It is hard to believe that posted information, and personal information collected in the course of online transactions on SNS sites, will not be used for any other purpose than promoting personal interactions between users and their "friends". Some SNSs (Facebook and BEBO) offer customers an option to opt-out of receiving advertising or services from third parties.

Principle 11 – Information must not be disclosed unless the agency believes the disclosure is directly related to the purposes for which it was collected, with certain exceptions. Acceptance of disclosure is a precondition for use of SNSs and therefore authorized by the user. There is an ambiguity here. The agency and the customer or user may differ in their respective understandings of the purpose for which the information was disclosed. The question arises whether customers would be agreeable in all cases for their information to be provided for all the purposes decided by the SNSs or their "trusted affiliates". If they cannot make that unconditional commitment, they should not use the service.

It is important to note that once data has been handed over to a third party new privacy and terms of use statements govern how the data is used. Once transferred the information is subject to incalculable manipulations. While the SNS has no obligation to check how their data is being used, moral practice would suggest that checks be carried out in the best interests of their users.

Principle 12 – An agency must not assign a unique identifier to an individual unless it is necessary for carrying out agency functions. None of the privacy statements refers to the use of unique identifiers. It is unsurprising that no SNS addressed Principle 12 in its privacy statement because there are risks to privacy from using unique identifiers and also from not using unique identifiers. The risk in using a single unique identifier across multiple information collections is that unrelated information about an individual could be used out of context. However, if social security or income tax numbers or other unique identity numbers are collected as part of the personal information posted to SNSs then this could be a problem area for privacy considerations. In New Zealand, the lack of a single unique identifier, such as a social security number or national identity number, means that New Zealand citizens are less vulnerable to privacy invasions and identity theft than their counterparts in the United States, for example.

5. Discussion

Most terms of use and privacy statements on SNS websites simply provide exculpatory clauses to ensure that the SNSs are not vulnerable to litigation in terms of national information handling legislation. SNSs want to be seen to be law-abiding and socially responsible organisations, without themselves being held legally responsible. Many of them operate out of the United States where their state or federal laws may specify legal constraints or obligations inimical to the operation of their services. Accordingly, they are unanimous in requiring users, visitors or members to accept that risks of site use belong to the user alone. The SNSs place contractual responsibility for consequences of SNS use squarely on the user.

For most users the main concerns relate to their proprietary rights to information posted on their profiles. Here the waters become quite murky. For example, the Twitter "terms of service" state that "you retain your rights to any content you submit" and that "what's yours is yours – you own your content". Bebo and Facebook similarly state that the user owns their information, but that the user grants to them the right to use, process and otherwise distribute that information. For example, Habbo's "terms and conditions" state that the user grants to Sulake, Inc (owners of Habbo website and services) "…the unrestricted, unconditional, unlimited, worldwide, irrevocable, perpetual fully paid and royalty free right and licence to host, use, copy, distribute, reproduce disclose sell, re-sell, sub-licence, display, perform, transmit, publish, broadcast… or otherwise exploit in any way whatsoever, all or any portion of your user content…" These terms of use statements are very similar to that of LinkedIn. Bebo, on the other hand assumes a "limited licence to use, modify, publicly perform, publicly display, reproduce and distribute" users material. On the Twitter "terms of service" page appears the statement "All right, title and interest in and to the services (excluding content provided by users) are and will remain the exclusive property of Twitter and its licensors". The distinction between content and services becomes confusing when one looks at the Twitter Privacy Policy which states "by using our Site you are consenting to our processing of your information as set forth in this Privacy Policy

now and as amended by us. "Processing" means using cookies on a computer or using or touching information in any way, including, but not limited to, collecting, storing, deleting, using, combining and disclosing information. All of which activities will take place in the United States." However, the concern of this investigation is not with proprietary rights to posted information so much as to the protection of users' privacy and information handling rights as specified in the New Zealand Privacy Act.

Among the risks involved in using social network services is the sale of personally identifiable information to third parties (Govani & Pashley, 2007). Data brokers, for example, compile consumer information from a variety of public and private sources and then offer it for sale to different entities for a range of purposes. In the United States, even government agencies purchase consumer information from data brokers for law enforcement and other purposes (President's Task Force on Identity Theft, 2007) A wide range of sources can be exploited by data brokers to garner the information they sell. Those that may not operate in an entirely legitimate fashion also open the doors for criminals. Once they obtain victims' personal information, criminals can misuse it by opening new accounts in the victim's name, accessing the victim's existing accounts, or using the victim's name when arrested. Recent survey data show that misuse of existing credit accounts, however, represents the single largest category of fraud (President's Task Force on Identity Theft, 2007). Govani and Pashley (2007) found that the majority of students were aware of the ability to restrict the amount of information they provided to different Facebook users. While 40% of users restricted some of their information, large numbers shared personal information like cell phone numbers and home addresses. They concluded that users "generally feel comfortable sharing their personal information in a campus environment" (Govani & Pashley, 2007). Participants said that they "had nothing to hide" and "they don't really care if other people see their information." Earlier research has shown that many online users of services, such as online banking, online purchasing and other interactive websites, are prepared to forgo the protection that would normally be a part of commercial transactions for the convenience of using the online functionality (Oermann & Dittmann, 2006; Yau, 2007). It is axiomatic that the use of social networking services is driven by peer-group pressure, which provides an environment of "value congruence" as described in Cazier's (2006) research. Such peer-group pressure is particularly important to younger people who are more likely to be concerned with belonging to the group than by concerns for privacy issues in later life. Providing information about dates and places of birth, names of parents and grandparents or other family members, often unwittingly, can result in this information being used for purposes of identity theft, if not immediately, then in future years. Youthful carelessness or misdemeanours can be recorded and accessed for future use in ways that cannot be currently anticipated. As has been argued above, the principles driving national legislation are a reflection of the values and concerns of the nations concerned. Legislation tests those values by wide consultation prior to enactment. National legislation on privacy and data communication therefore forms a lens through which one could consider whether internet websites conform to national values, providing a framework for evaluating websites. However, when the users of a social networking service make use of that service, they agree to abide by the terms of use of the service concerned, and in doing so enter into a contract outside of the protection offered by national privacy or data communications legislation.

Accordingly, one can conclude that the use of legislative principles as a means of evaluating website privacy statements and "terms of use" highlights the shortcomings of the contract in protecting users and their personal information. The privacy statements and "terms of use" are shown to be written more for the legal protection of the hosting organisation than to provide assurance to users about the manner in which their personal information will be handled **(**Papacharissi & Fernback, 2005). Such protection of the social networking site from litigation calls into question the business integrity of these services and justifies further investigations of this nature. At very least it raises the question of whether such sites have a corporate responsibility for the protection of their customers – and indeed, who their real customers are. The value of the principles of the New Zealand Privacy Act as a checklist for people wishing to evaluate business integrity and the social responsibility of social networking sites has been highlighted.

6. Conclusions

One may conclude that, at least in the case of New Zealand, the principles articulated in the New Zealand Privacy Act form a useful template for evaluating ethical information handling practices of internet businesses. Nevertheless, two further issues emerge. In a blog article dated 23rd September, Bruce Schneier (2009) reported on an Illinois district court that allowed a couple to sue their bank for

failing to secure their account sufficiently. The principle involved was that the person with the ability to mitigate the risk is responsible for the risk. On the basis of this principle SNSs could be held accountable in certain jurisdictions for any misuse of personally identifiable information through their websites. SNSs should specify precisely what use is made of user information. Detailed and specific statements about their information handling policies would ease public concerns about ethical information handling and encourage the emergence of the benefits of value congruence as articulated by Cazier (2006). A second, more significant issue is the doubt that is emerging about trust as a factor in internet transactions. Although people have been warned of the risk and the longer term consequences that might follow, in order to participate in desired group activities such as are manifested in SNSs, individuals are prepared to risk their personally identifiable information. This appears to be a human behaviour pattern that is far deeper seated than concepts of trust and privacy. Further research in this area could lead to a new way for internet commerce to reach out to customers. It could also result in a better understanding of how to ensure the well-being of people when using the internet.

7. Appendix 1: Analysis of selected social networking service "terms of use" and privacy statements

Feature	Provision	Twitter	Habbo	MySpace	LinkedIn	Bebo	Facebook
Principle 1	Lawful, necessary collection	Yes	Yes	Yes	Yes	Yes	Yes
Principle 2	Information directly sourced	Yes	Yes	Yes	Yes	Yes	Yes
Principle 3	Owner advised of collection	Yes	Yes	Yes	Yes	Yes	Yes
Principle 4	Lawful, fair and un-intrusive collection	Yes	Yes	Yes	Yes	Yes	Yes
Principle 5	Protection against loss	No	No	No	No	No	No
	Protection against un-authorised use.	No	No	No	No	No	No
	Confidentiality	No	No	No	No	No	No
Principle 6	Right to view personal information held	No	No	Yes	Yes	No	Yes
Principle 7	Can request correction	Yes	Yes	Yes	Yes	Yes	Yes
	Request correction confimation	No	No	No	No	No	No
	User informed of disclosure	No	No	No	No	No	No
Principle 8	Accuracy checked	No	No	No	No	No	No
Principle 9	Information held only while necessary	No	No	No	No	No	No
Principle 10	Information used for collected purpose	No	No	No	No	No	No
Principle 11	Permission required for disclosure	No	No	No	No	No	No
Principle 12	Use of unique identifiers	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown

References

Barnes, S.B. (2006) "A privacy paradox: Social networking in the United States", *First Monday*, Vol 11, No 9. (Retrieved August 30, 2009, from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312)

Bialek, A.R. and Smedresman, S.M. (2008) "Internet Risk Management: A Guide to Limiting Risk Through Web Site Terms and Proactive Enforcement", *Intellectual Property & Technology Law Journal,* Vol 20, No 11, pp 1-15.

Blaikie, N. (2007) *Approaches to social enquiry* (2 ed.) Cambridge, UK: Polity Press.

Boyd, D.M. and Ellison, N.B. (2007) "Social Network Sites: Definition, History, and Scholarship", *Journal of Computer-Mediated Communication,* Vol 13, No 1, pp 210-230.

Bruce, L. and Berg, M. (2001) *Qualitative research methods for the social sciences*, Allyn and Bacon, Needham Heights, MA.

Cazier, J. A. (2006). *Value congruence and trust online,* Cambria Press, Youngstown, N.Y.

Cazier, J. A., Wilson, E. V., & Medlin, B. D. (2002). "The role of privacy risk in IT acceptance: An empirical study." *International Journal of Information Security and Privacy,* Vol 1, No 2, pp 61–73.

Cazier, J. A., Shao, B., & Louis, R. (2007). "Sharing information and building trust through value congruence". *Information Systems Frontiers,* Vol 9, No 5, pp 515-530.

Chiaramonte, P., & Martinez, E. (2006). *Jerks In Space*. The New York Post. New York.

Creswell, J.W. (2009) *Research design: Qualitative, quantitative and mixed methods approaches* (3d ed.) Sage Publications, Thousand Oaks, CA.

Dwyer, C., Hiltz, S.R., & Passerini, K. (2007, August 09 - 12). "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace", Proceedings of the Thirteenth Americas Conference on Information Systems, Keystone, Colorado.

Ecole Polytechnique de Montreal. (2001). "Glossary". [online] http://www.erudium.polymtl.ca/html-eng/glossaire.php

Edwards, J.R., & Cable, D.M. (2009). "The Value of Value Congruence". *Journal of Applied Psychology,* Vol 94, No 3, pp 654–677.

Fernandez, P. (2009) "Online Social Networking Sites and Privacy: Revisiting Ethical Considerations for a New Generation of Technology", *Library Philosophy and Practice*, pp 1-10. [online] http://digitalcommons.unl.edu/libphilprac/246/#

Govani, T. and Pashley, H. (2007) *Student awareness of the privacy implications when using Facebook.* [online] http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf

Gross, R. and Acquisti, A. (2005) "Information Revelation and Privacy in Online Social Networks", Proceedings of the 2005 ACM workshop on Privacy in the electronic society, pp. 71-80, ACM, Alexandria, VA.

Haythornthwaite, C. (2005) "Social networks and Internet connectivity effects", *Information, Communication & Society,* Vol 8, No 2, pp 125-147.

Hodge, M.J. (2006) "The Fourth Amendment and privacy issues on the "new" Internet: Facebook.com and MySpace.com", *Southern Illinois University Law Journal,* Vol 31, pp 95-122.

Holsti, O, (1968) "Content analysis". In G. Lindzey and E. Aaronsfield (Eds.) *The handbook of social psychology,* pp 596-612, Addison-Wesley, Reading, MA.

Hoofnagle, C. J. and King, J. (2008). "What Californians understand about privacy online". [online] http://ssrn.com/abstract=1262130

Kolbitsch, J. & Maurer, H. (2006). "The Transformation of the Web: How Emerging Communities Shape the Information we Consume". *Journal of Universal Computer Science*, Vol 12, No 2, pp 187-213.

Kornblum, J. and Marklein, M, B. (2006) "What you say online could haunt you". [online] http://www.usatoday.com/tech/news/internetprivacy/2006-03-08-facebook-myspace_x.htm

Krippendorf, K. (1980) *Content analysis: An Introduction to its Methodology*, Sage Publications, Beverley Hills, CA.

Kruck, S.E., Gottovi, D., Moghadami, F., Broom, R., and Forcht, K.A. (2002) "Protecting personal privacy on the Internet". *Information Management & Computer Security,* Vol 10, No 2, pp 77-84.

Luo, X. (2002) "Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory", *Industrial Marketing Management,* Vol 31, No 2, pp 111–118.

Meinert, D.B., Peterson, D.K., Criswell, J.R., and Crossland, M.D. (2006) "Privacy policy statements and consumer willingness to provide personal information", *Journal of Electronic Commerce in Organizations*, Vol 4, No 1, pp 1-17.

Myers, M.D. (2009). *Qualitative research in business and management.* Sage Publications, Thousand Oaks, CA.

Newman, K.I and Nollen, S. D. (1996). "Culture and congruence: The fit between management practises and national culture". *Journal of International Business Studies*, Vol 27, No 4, pp 753-779.

New Zealand Privacy Act (1993). [online] http://www.privacy.org.nz/legislation/1993028/toc.html.

New Zealand Privacy Commissioner. (n.d.) *The Privacy Act and Codes*. [online] http://www.privacy.org.nz/privacy-act/

Oermann, A., and Dittmann, J. (2006) "Trust in e-technologies". In M. Khosrow-Pour (ed.) *Encyclopedia of E-commerce, E-government, and Mobile Commerce,* pp 1101-1108, Idea Group, Hershey, PA.

Orlikowski, W.J., & Baroudi, J.J. (1991) "Studying information technology in organisations: research approaches and assumptions". *Information Systems Research,* Vol 2, No 1, pp 1-28.

Papacharissi, Z., & Fernback, J. (2005). "Online privacy and consumer protection: an analysis of portal privacy statements". *Journal of Broadcasting and Electronic Media*, Vol 49, No 3, pp 259-282.
Pollach, I. (2005) "A typology of communicative strategies in online privacy policies: ethics, power and informed consent", *Journal of Business Ethics*, Vol 62, No 2, pp 221-235.
Preibusch, S., Hoser, B., Gürses, S., and Berendt, B. (2007) "Ubiquitous social networks – opportunities and challenges for privacy-aware user modeling", Data Mining for User Modeling Workshop, Proceedings of the 11th International Conference, UM 2007, Corfu, Greece, July 25-29, 2007.
President's Task Force on Identity Theft. (2007) *Combatting identity theft: A strategic plan.* Federal Trade Commission, Washington, D.C..
Rauhofer, J. (2008) "Privacy is dead, get over it! Information privacy and the dream of a risk-free society", *Information & Communications Technology Law,* Vol 17, No 3, pp 185-197.
Schneier, B. (2009) "Eliminating Externalities in Financial Security", *Schneier on Security: A blog covering security and security technology,* [online] http://www.schneier.com/blog/archives/2009/09/eliminating_the.html
Slane, B. (2001). "Small investment, big return". [online] http://www.privacy.org.nz/sfinf.html .
Slane, B (n.d.) "Privacy Laws and the Private Sector". [online] http://www.privacy.org.nz/library/privacy-laws-and-the-private-sector.
Smith, T. (2009) "The social media revolution", *International Journal of Market Research,* Vol 51, No 4, pp 559-561.
Stahl, B. C. (2004). "Responsibility for information assurance and privacy: A problem of individual ethics?" *Journal of Organizational and End User Computing*, Vol 16, No 3, pp 59-77.
Wang, Y.D., & Emurian, H.H. (2005). "Trust in e-commerce: Consideration of interface design factors". *Journal of Electronic Commerce in Organizations*, Vol. 3, No. 4, pp 42-60.
Weiss, S. (2009) "Privacy threat model for data portability in social network applications", *International journal of Information Management,* Vol 29, pp 249-254.
Zorn, R. (2006). "How to protect your privacy online". *The Dominion Post*, (18 November), p 19.

