Empirical Study of Privacy Issues among Social Networking Sites

Joanne Kuzma
University of Worcester, UK
j.kuzma@worc.ac.uk

Abstract: Social media networks are increasing their types of services and the numbers of users are rapidly growing. However, online consumers have expressed concerns about their personal privacy protection and recent news articles have shown many privacy breaches and unannounced changes to privacy policies. These events could adversely affect data protection and compromise user trust, thus it is vital that social sites contain explicit privacy policies stating a comprehensive list of protection methods. This study analyzes 60 worldwide social sites and finds that even if sites contain a privacy policy, the site pages may also possess technical elements that could be used to serendipitously collect personal information. The results show specific technical collection methods most common within several social network categories. Methods for improving online privacy practices are suggested.

1 Introduction

With the increase in global Internet sites, online social networks (OSNs) are gaining increased importance to many people around the world for both work and leisure (Preibusch, et al, 2007). However, as these sites grow in popularity, they face a variety of design and legal challenges, especially factors related to privacy protection and misuse of user data. Studies have shown that online consumers are concerned about how OSNs protect their personal information, so it makes sense for site owners to provide privacy policies indicating various methods the firm uses to protect personal data and provide consumer protection. Because sites have not always been proactive in providing strong protection, industry groups have created voluntary protection standards and some governments have enacted legislation protection.

This research analyzes the level of privacy protection among 60 major OSNs throughout the world. It aims to answer the following research questions:

1. Are there common privacy factors that are being neglected by OSNs?
2. Is there any relationship between sites that cater to specific geographic markets in dealing with privacy issues?
3. Do some categories of OSNs (based on geography) have more privacy criteria problems than others?

The study starts with a literature review of the market for OSNs and how online consumers view privacy and trust. It also reviews types of privacy factors, legal and industry standards and concludes with prior studies of online privacy protection. Next, the research methodology is covered, followed by an explanation of the survey results. Finally, implications for the findings are highlighted, along with suggestions for OSN site owners to consider when strengthening their policies.

2 Literature Review

2.1 Growth of Social Sites

The growth of the Internet technologies has led to an explosion of OSNs, including Facebook and YouTube. Communication channels and tools on these sites can include blogs, email, wikis and other methods consumers use to communicate with others all over the world, which has contributed to their phenomenal growth. In 2008, their use grew 35 percent in Europe, and 56 percent of the online European population visited these sites. The number of European users is expected to grow from 41.7 million to 107.4 million in the next four

years (Europa, 2009). According to Datamonitor (2007), in 2007 Asia Pacific users accounted for 35 percent of the social-networking memberships, Europe, Africa and the Middle East are 28 percent, North America 25 percent and Latin America at 12 percent.

The importance of OSNs has grown due to the advantages to both individuals and businesses. For individuals, they offer the opportunity to better network with others all over the world and organize their social life. According to Europa (2009), businesses can benefit from OSNs by serving different audiences with minimal financial effort. Firms can improve customer services and client involvement in product innovation and services, and can use communications technology to empower their own employees. Preibusch et al (2007) also indicate that OSNs use data mining techniques to collect information for marketing purposes, which eventually helps the business investments and financial profitability.

2.2 Consumer Privacy and Trust

According to Desai (et al, 2003) a study by Harris Interactive and the Privacy Leadership Initiative, 40 percent of Internet users claim privacy and security concerns kept them from buying things online. However, although the online audience is highly concerned about privacy of their data, these same users sometimes posses a dichotomy on their actual usage of privacy matters compared to what they indicate in surveys. According to Desai (et al, 2003), most people take increasing infringement on privacy as the price for living in the twenty-first century. The authors give a quote from cryptographer Bruce Schneier "If McDonalds offered a free Big Mac in exchange for a DNA sample, there'd be lines around the block."

Also, studies have shown that even when privacy policies exist, users don't always read them. A 2009 study of 2,500 worldwide OSN users found that only 45 percent read the privacy policy (Levin & Abril, 2009). Different customers may also have different expectations and attitudes towards privacy versus customer service. According to Hung & Wong (2009) some people may be disturbed about invasion of privacy while others welcome a firm's activities where sharing personal data may help the firm to provide better customer service.

While customers may accept some forms of risk when participating in online activities, it behooves businesses to create a climate whereby their users perceive that such risk is reduced, while the level of online trust is increased. Firms may accomplish this by implementing strong privacy policies on their sites (Hooper & Vos, 2009).

Preibusch et al (2007) show that although OSNs have individual privacy functions, these do not often deal well with the 'network' effects of data sharing. For example, if one user reveals specific data about himself as well as a list of friends, this 'network' information could lead to revelations about his friends that his friends had not intended. The authors further explain that leaks could be disastrous for individual users, who may lose trust or

leave the OSNs. This could lead for financial troubles for the OSNs who are trying to create marketing campaigns based on user data.

Not only do individual consumers express concerns about online privacy and trust, businesses also deal with these concerns. A 2009 study by Deloitte of 500 business executives reviewed firm's concerns on employee's use of social networking sites, blogs and other Web 2.0 technologies. The study found that employers are concerned with negative posts of their employees on these sites, and disclosure of sensitive or confidential information, thus damaging the firm's reputation or causing financial damage (EHSToday, 2009).

2.3 Data Collection Mechanisms

One of the research questions for this study was to determine if some OSN sites have more privacy criteria problem than others. This cannot be answered without a definition of what sort of privacy problems that consumers may encounter when perusing OSN sites. Firms may use a variety of technologies and mechanisms to collect personal data about consumers. Each of these poses concerns to consumers, and although social sites cannot prevent all data collection, OSNs could mitigate some level of user concern by revealing how the site uses these technologies. This information could be contained in an overall privacy policy page contained as a link on a prominent place on the home page. McRobb & Rogerson (2004) state that it is vital for organizations to publish a privacy statement policy on their site to reassure customers and to help build branding and image.

Hinduja (2004) explains that cookies were developed so a site could generally identify a visitor and keep track of how many times one visited the site. The author explains that controversy arises when a cookie is used as a pointer to a database of sensitive information, such as the number of times one has accessed a Web page, past browsing behavior within a site, and personal information voluntarily given when registering for the content. According to Bowie & Jamal (2006) another issue of cookies is that third-party sites can also gain information about the visitor. Turow (2004) indicates that 40 percent of people browsing the Web are unaware that cookies are a key component of data sourcing and they can be used to track online actions and compromise privacy. The European Union Data Protection Authorities recommend in Article 29 of the Working Party on Online Social networking that users are given the opt out choice and are warned of the privacy risks and on the personal data that is being made available to others, thus providing some protection against third-party collection (European Digital Rights, 2009).

A site should contain a link to the Platform for Privacy Preferences (P3P). This is a standardized set of best practices that describe a site's privacy practices. OSNs which implement these standards and policies indicate that they participate in good privacy practices, as well as making them available for consumers to easily review (W3C, 2007). Sites often use electronic files, called Web beacons, to allow the site to count the number of users or access information within cookies. Although OSNs are among the Web operators that use beacons, their implementation is not without controversy. Facebook incurred the wrath of its members over using beacons for an advertising system that sent information about member's shopping habits and other activities to Facebook. The beacons also allowed targeted advertisements to be sent to members (Nielsen, 2009).

2.4 Legal Standards

A major problem OSNs face is understanding and complying with a myriad of privacy laws and regulations. Firms around the globe may be subject to different and even conflicting laws, or lack of them. In order to protect user's information such as names, addresses and other sensitive data, some governments have developed regulatory measures. According to Gunasekara & Toy (2008), the European Union developed a Privacy Directive and "Safe

Harbor" regime that allows U.S. companies to collect personal data related to European Union citizens. The Asia-Pacific APEC Privacy Framework is another regime covering Asian data privacy. Member of the Gulf Corporation Council (Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the UAE currently have no regulations dealing with privacy or privacy issues in general (Shalhoub, 2006). The U.S. has a myriad of privacy laws including Children's Online Privacy Protection Act, which protects children's data, the Gramm-Leach-Bliley Act covering financial information and the Health Insurance Portability and Accountability Act which protects consumer's health information (Phillips, 2004).

There have been lawsuits over privacy issues associated with OSNs. According to the Associated Press, in 2009 Facebook users in California filed suit against the firm accusing it of violating state privacy laws and misleading users about how personal information is used. According the article it may be difficult for a jury to decide how realistic privacy expectations can be when people are overly forthcoming about details of their personal lives (Casale, et al, 2009).

2.5 Studies of Social Sites

A 2009 University of Cambridge study of 29 social sites, including Facebook and MySpace, found that the majority of sites did contain a privacy policy. However, this study found that many did not make their policies prominent when soliciting users to sign up. The sites avoided promoting the policy for fear of putting off potential members, thus encouraging users to share data with impunity (Social Networks, 2009). A study of privacy policies in nine countries found that privacy policies are more commonly found where customers have greater access to and experience using Web sites and countries where there are more established privacy laws (Johnson-Page & Thatcher, 2001). Fernandez, P. (2009) indicates some OSNs, like Facebook, may provide adequate privacy terms of agreement. However, users can use sites like Facebook to create other applications shared by users which could exploit or expose user information. These associated applications may not provide privacy setting as strong as Facebook or other social sites.

A study by Dwyer (et al, 2007) of Facebook and MySpace found that perceptions of privacy and trust were similar to members of both OSNs, and they had similar concerns of privacy. However, an interesting result of their study demonstrated that young adults were still open to use the sites and build online relationships even if they perceived trust and privacy safeguards were weak.

Levin & Abril (2009) completed a study of 2,500 young adults on their expectations of privacy on OSNs. Found that online members do expect some level of privacy within the network. However, they found that OSN privacy policies and terms of service rarely adequately protect the dignity of members, even though they are well-positioned to do so with technologies available. The authors also indicate that some OSNs may work with national government entities to enhance their privacy protection. For example, Facebook has collaborated with the Ontario Canada Information and Privacy Commissioner to publish privacy guidelines.

3 Methodology

The research in this paper was accomplished through analyzing 60 OSNs to determine the levels of privacy protection. The project consisted of three phases:

1. Choosing a testing tool
2. Choosing a list sites to test
3. Running the test and analyzing results

3.1 Choosing a Testing Tool

The first phase of this study was to choose a privacy testing tool, and several criteria were used to select it. Firstly, due to budget constraints, cost was an issue. It was preferable to either find a free testing tool or one with minimal cost (under $100). Second, because the researcher's PC would be used to testing, the product either had to be installed and run on a Microsoft XP operating system, or had to be an online testing tool. Third, the product's functionality had to be robust enough to check a variety of privacy factors including whether a site had a privacy policy, web beacons, cookies and third-party links.

An online P3P validation tool from W3C was reviewed. Although the tool was free and did not require any software installation (W3C, 2010), it was limited in the functional results it produced, and did not provide information about cookies, web beacons and links. IBM's product Rational Policy Tester Privacy Edition collected a wide variety of privacy information in its reports, including regulatory compliance data (IBM, 2010). However, its cost of $3,610 was beyond the affordability for the research. Erigami's online testing tool, Truwex Online Tool, is a free product that Web developers could use to review privacy standards and several regulations, such as US Children's Online Privacy Protection Act (COPPA). Its reporting format collects privacy information such as:

- **Tracking third party content such as cookies and Web beacons.**
- Visitor tracking by cookies and Web beacons.
- P3P policy usage.
- PII analysis such as Web forms that collect names
- Compliance with COPPA laws
- Privacy policy hyperlinks (Erigami, 2008a)

Truwex also has other features, such testing Web accessibility and site quality factors, but those options were not relevant for this research project. Because of the robust information produced and the free availability to use, this product was chosen for testing. This software has been used by other researchers to analyze government Web sites. In the spring of 2008, the Government of Saskatchewan, Canada used Truwex 2.0 to evaluate perform Web accessibility testing (Wu, 2008).

3.2 Choosing a List of Sites to Test

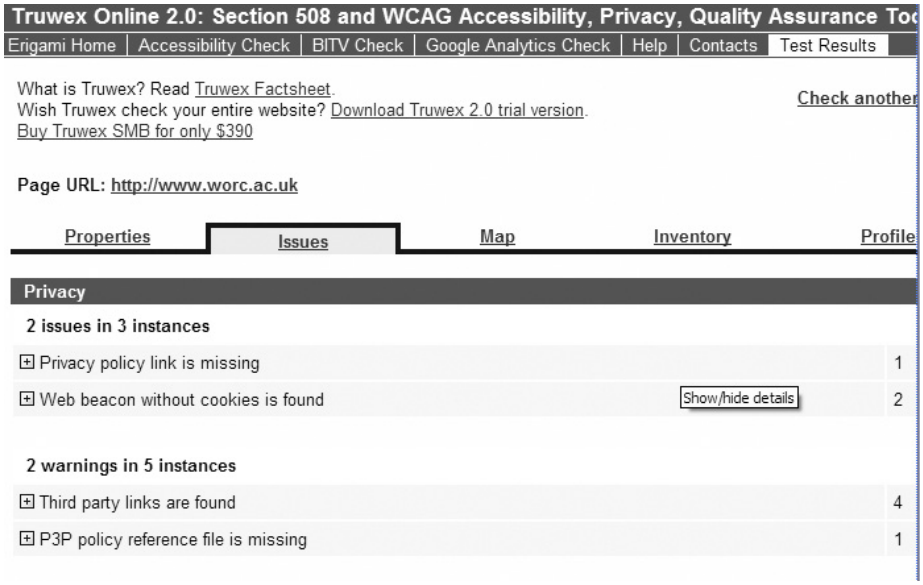
The second phase of this project was to select 60 OSNs in four different categories. To review a list of world-wide sites, the list was drawn from four main geographical regions: a) Asian, b) European, c) Latin American and d) Worldwide sites. From each of these areas, 15 of the most highly visited OSNs were chosen and tested. It was vital to discover which social site was most prevalent within each of the categories. To determine which social site should be aligned within each of the four geographical areas, it was necessary to analyze which country the majority of visitors used the site. A global digital marketing intelligence firm, comScore, provided studies about OSNs throughout the world. For example, a study regarding consumer visits to social site Bebo indicates that 62.5 percent of visitors came from Europe (comScore, 2007). Thus, the Bebo site was included within the "European"

category. If a site was more evenly distributed throughout the world, it was included within the "Worldwide" category. According to comScore studies (2007), 15 percent of visitors for H15 are located in North America, 24 percent in Latin America, 31 percent in Europe, 21 percent in Asia and 9 percent in other areas. Therefore, this was considered to be a 'worldwide' social site.

3.3 Running the Test and Analyzing Results

To use the Truwex product, the researcher inserted each social site's Uniform Resource Locator (URL) into an online selection box, and chose the 'privacy' function option. The tester then received a detailed compliance report, shown in Figure 1. This report divided a privacy test into two parts: serious privacy issues which should be immediately fixed to comply with industry standards, and warnings, which should be reviewed but are not considered critical to privacy protection. Figure 1 shows that for this test site, there are two different serious concerns. First, the site does not have a privacy policy link. Second, there are two pages are found with Web beacon without cookies. Two less-serious warnings are found: third party links and P3P policy reference file is missing.

Figure 1: Truwex Screen Print



For this test, the researcher inserted each of the 60 individual site URLs into the tool and ran the report. Raw data was compiled into an Excel spreadsheet for later detailed analysis. For this test, the researcher encountered one problem that required manual review. For some sites that were not in English, Truwex results showed that a privacy page did not exist. This may have occurred for several reasons. Firstly, for the site vistu.com, the site language was Spanish and the privacy page was named 'Privacidade'. Second, an issue occurred where the privacy information could have been stored within a non-privacy page. For example, the site taobao.com had the privacy information contained within the 'legal notices' page and Nicovideo had its privacy information within the 'terms of use' page. Therefore, the researcher manually reviewed all sites where Truwex indicated that no there was no privacy policy on the site. There were eight sites that had privacy information contained within other pages.

4 Results

Raw data for this study was compiled and placed into four worldwide categories. Table 1 shows results of Asian privacy results, while Table 2 shows results for Europe, Table 3 for Latin America and Table 4 contains data for worldwide sites. Each table contains privacy data for 15 specific OSNs related to that category. For each site, eight privacy criteria were compiled:

- Privacy policy missing
- Web beacon with cookies found
- Web beacon without cookies found
- Third party cookies found
- PII: page collects personal information identifier
- Form with method get is used
- Third party links found (warning)
- P3P policy reference file missing (warning)

The first six criteria are considered 'critical' privacy issues, and can cause serious problems with privacy protection. The last two criteria (G and H) are merely privacy concern warnings, and are not critical to privacy protection, but designers should still review these issues. For several criteria, only one outcome could be produced for each Web site. For example, column A (privacy policy missing) and column H (P3P policy reference file missing) could either have a result of zero or one for each site. However, the results from other columns could show large aggregate numbers across all pages for that site.

Results of Table 1 show that most Asian sites did contain a privacy policy, but two of them (QQ and baidu) did not. Most sites (11 of 15) do not contain the P3P policy reference file. The most critical problems for Asian sites were the large number of Web beacons without cookies (372 total). All sites but one (baidu) had these privacy issues, with the nicovideo containing the greatest number of problems (105 throughout the site).

Table 2 shows the results for European sites, with two sites not possessing a privacy policy (faceparty and Dol2day). The number of total pages containing Web beacons without cookies was 266, with skyrock (86) and hyves (47) containing the greater number of issues. Five sites did contain third-party cookies, another critical issue. Most OSNs did have both types of warnings (categories G and H).

Latin American sites (shown in Table 3) all had privacy policies. All sites but two had serious problems with 'Web beacon without cookies found' (272 pages). Five sites possessed third party cookies for a total of 35 different pages. All sites but one had third party link warnings (128 total warnings). Table 4 results for worldwide

2

OSNs revealed that all sites but two had issues with Web beacons and six sites displayed third-party cookies.

Table 1: Asian Social Site Privacy Results

	Country	A	B	C	D	E	F	G	H
QQ	China	1		34			1	99	1
baidu	China	1						2	1
taobao	China		2	47	5			27	1
sohu	China		2	34	2		1	422	1
Fc2	Japan		1	9	8			1	1
nicovideo	Japan			105			1	41	1
Livedoor	Japan			3			4	14	1
naver	Korea		1	3	3		1	27	
daum	Korea			74			1	6	
nate	Korea		1	3	1		2	52	
empas	Korea			4			2	53	
friendster	Asia			1		1	1	2	1
xanga	Asia			21				209	1
bigadda	India			32		1		8	1
ibibo	India			2	1			2	1
Total		2	7	372	20	2	14	965	11

Table 2: European Social Site Privacy Results

	Country	A	B	C	D	E	F	G	H
Badoo	Europe			2		1			
Netlog	Europe			7				3	1
Faceparty	UK	1		2			1	1	1
Studivz	Germ			2		1		3	1
Wasaibi	France		2	16	9	1	1		1
Skyrock	France		1	86	2	1	2	18	1
Jux	Germ		2	11	2	1	1	2	1
Wkw	Germ			24				6	1
Lindernau	France			1		1	1	7	1
Trombi	France		1	1	1	1		7	1
Bahu	France			8			1	1	1
Lexode	France		4	16	6		1	14	1
Tuenti	Spain					1		1	1
Hyves	Nether			47				11	
Dol2day	Germ	1		3				4	1
Total		2	10	226	20	8	8	78	13

Overall, results from all four categories illustrated consistent findings across the various privacy issues and warnings. One positive is that most of the OSNs do contain some sort of privacy statement, with only 8 percent not exhibiting one. However, as was explained in the methodology section, some sites do bury their privacy statement within another page that may not necessarily be obvious to a consumer. The use of Web beacons is a prevalent problem among the majority of sites. Twenty sites (44 total pages) contained Web beacons with cookies while 54 sites (1079) had Web beacons without cookies. Third-party cookies were found in almost 37 percent of sites (22 total sites and 114 pages).The critical issue of PII collection was found in only two sites in Asia, while contained in eight sites in the other three categories. The issue of 'form with method get is used' was found in 43 percent of sites (26 total) with the Asian category including the greatest percent.

Table 3: Latin American Social Site Privacy Results

	Country	A	B	C	D	E	F	G	H
Migente	Latin		4	44	7	1		4	1
fotolog	SA			9			2	2	1
Sonico	SA			16		1		2	1
orkut	Brazil			3		1		5	1
8p.com.br	Brazil			5				4	1
multiply	Brazil					1			
Wamba	SA		5	21	14	1		24	1
metroflog	SA		1	5	4			1	1
clyclop	Latin			2			1	1	
quepasa	Latin			22		1		5	1
vostu	Latin						1	4	1
totalvenez	Venez		1	11	1		1	29	1
Totalurugu	Urugua		2	17	9		2	19	1
batepapo	Brazil			50		1		1	1
boliviabella	Bolivia			67		1		27	1
Total		0	13	272	35	8	7	128	13

Table 4: Worldwide **Social Site Privacy Results**

	Country	A	B	C	D	E	F	G	H
facebook	na			12		1		6	
Hi5	na		1	11	3	1	1	6	1
linkedln	na			2		1		1	1
myspace	na		1	21	2	1	1	5	1
twitter	na			21	1	1	1	3	1
bebo	na		2	18	4	1		3	1
habbo	na		4	17	10			4	1
tagged	na		6	51	19	1		2	1
youtube	na			25			2	24	1
couchsur	na			3					1
jaiku	na							1	1
kiwibok	na			15		1		4	1
itsmy	na							6	1
inviteshar	na	1		1			1	15	1
buzz	na			12				2	1
Total		1	14	209	39	8	6	82	14

Although the two columns of 'warning' data are not considered especially critical towards safe privacy practices, sites that contain these issues should still review their occurrences to determine if they should be corrected. Almost all sites (95%) had these warnings, with sites averaging 22 of these warnings each. Missing P3P

policy reference file was another common warning found in 85% of OSNs.

5 Implications and Recommendations

The purpose of this study was to determine the level of privacy protection gaps for worldwide users of OSNs. The data indicated there was a considerable variation in the types and amounts of privacy problems on various sites. Most sites did have some type of overall privacy policy (92 percent). The most serious issue 'web beacons without cookies' was found in 90 percent of sites with an average of 21 web beacons found in each. Other critical issues included: third party cookies found (37 percent of sites with an average of 5.2 per site), page collects PII (40 percent of sites), form with method get is used (43 percent with an average of 1.3 per site), and web beacons with cookies (33 percent with an average of 2.2 per sites). Non-serious warnings consisted of third party links (93 percent of sites and average of 22 per site) and P3P policy missing (85 percent).

One aim of this study was to analyze if there was a difference in privacy issues among sites in each of the four worldwide geographical areas. In most cases, for each of the privacy issue types, the numbers in the four areas did not show a great different. For example, for 'Web beacons without cookies,' there were 14 Asian and European sites with this problem, and 13 Latin American and worldwide sites, not a statistical different. The one category showing a marked difference was the issue with PII information collected. Only two Asian OSNs had this problem while eight European/worldwide sites and nine from Latin American had them, a significant difference.

Overall results suggest that even with industry standards and some local laws which mandate specific levels of privacy and data protection, there are still serious problems with OSNs collecting personal data through a variety of technical mechanisms. This could lead to potential problems with consumer trust and even lead to consumers abandoning the use of a site.

There are a variety of mechanisms that OSN site owners can use to provide effective privacy protection. But, one issue that should be addressed is why OSNs do not implement these mechanisms and develop strong privacy policies. One study interviewed Webmasters of 500 Fortune 500 sites that did not contain a privacy policy on the home page. They were asked why the business did not have a policy and other privacy protection mechanisms. The three main reasons for not providing a policy included: a) the policy was in development, b) a policy appears in the site of a business subsidiary and c) there is no strong need to have a policy and protection (Liu and Arnett, 2002). Thus, it is disappointing to discover that some site developers still feel privacy is not an important issue. This leads to the suggestion that site owners need to educate their staff on the importance of consumer trust to their financial bottom line as well as to industry privacy mechanism and legal mandates.

Site owners should realize there are financial implications for not adhering to strong privacy practices. Culnan & Milne (2001 and Fox et al (2000), as cited by Wirtz et al (2007) state that over 50 percent of internet users falsify or misrepresent data at least occasionally, and the likelihood of such behavior is higher when privacy concerns are high. Wirtz proposed these higher levels of privacy unease leads to data falsification, which results in erroneous or incomplete information within a firm's marketing database.

Levin & Abril (2009) indicate that technology and demand are in place for OSNs to provide stronger privacy protection through the use of privacy protection tools, procedures, and meaningful systems of dispute resolution. They also argue that if OSNs do not police themselves, governments will develop possible regulatory measures to protect against privacy breaches. It is imperative that OSNs develop internal processes and procedures to ensure that privacy protection is provided for during development of the Web sites and is periodically reviewed. Privacy protection is not merely a technical problem, but should be considered a multi-dimensional approach where industry standards, legislation, management processes and procedures, training and technology all play a role in enhancing consumer trust in online commercial sites.

The research in this study could be further expanded to analyze a variety of other issues and factors related to privacy of OSN sites. First, it would be helpful to understand which privacy elements users find most helpful and relevant when they review an overall privacy policy. This would not only be appropriate for the OSNs, but also to online sites for other industries. For example, a 2002 study of consumers of online health care sites found that opt-in and opt-out privacy elements were more important than the overall site's privacy policy (Earp & Baumer, 2003). Knowledge of privacy preferences would allow sites to tailor privacy policies and procedures to those factors that their users find most appropriate. A second way to expand this research would be to analyze other privacy elements which may or may not be contained within a site. For example, elements such as the ability for consumers to opt-in or opt out could also be reviewed.

6 Conclusion

This study has shown that even with industry standards and some legal mandates among various countries, certain privacy elements are not strongly supported among OSNs. This has the possibility of adversely affecting these sites, as the number of OSN sites is growing and consumers have greater options to access alternative methods of social networking.

Consumers have shown increased concerns on data security and collection by OSNs. To deal with these issues, industry groups have established technical standards and guidelines sites should follow when dealing with privacy issues, such as mandating that all sites have a privacy policy. In addition, some countries have started to enact specific privacy laws, although this is not globally universal. But, even with these actions, the results of this study show that popular OSN sites contain a variety of critical and non-critical privacy elements that put consumer's private data at risk. Site owners should realize that this could increase consumer's distrust, and even lead to financial and marketing problems for the firm. Instead, firms should use a multi-dimensional approach including technical, managerial and training to address online privacy and provide their consumers with higher levels of privacy protection.

References

1. Bowie, N. & Jamal, K. (2006) Privacy Rights on the Internet, Self Regulation or Government Regulation, *Business Ethics Quarterly,* Volume 16 (Issue 3), 323-342.
2. Casale, J., Greewald, J., Hofmann, M. & Roberts, S. (2009) Friends Request Privacy From Site, *Business Insurance*. Volume 43 (Issue 29), 23.

3. comScore (2007) Social Networking Goes Global, comScore.org, Retrieved March 3, 2010, from http://comscore.com/Press_Events/Press_Releases/2007/07/Social_Networking_Goes_Global.
4. Datamonitor (2007) Social Networking's Explosive Growth to Plateau in Five Years, Retrieved March 20, 2010, from http://www.marketingcharts.com/interactive/social-networkings-explosive-growth-to-plateau-in-five-years-2102/datamonitor-us-social-networking-membership-sharejpg/.
5. Desai, M., Richards, T. & Desai, K. (2003) E-commerce policies and customer privacy, *Information Management & Computer Security*, Volume 11 (Issue 1), 19-27.
6. Dwyer, C., Hiltz, S., Passerini, K. (2007) Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace, *In: Proceedings of the Thirteenth Americas Conference on Information Systems, August 9-12, 2007*, Keystone, CO. USA. Retrieved March 3, 2010, from http://csis.pace.edu/~dwyer/research/DwyerAMCIS2007.pdf.
7. Earp, J. & Baumer, D. (2003) Innovative web use to learn about user behavior and online privacy, *Communications of the ACM*, April 2003, Volume 46 (Issue 4), 81–83.
8. EHSToday (2009, November) Managing the Web 2.0: Social Networking Policies, Retrieved March 5, 2010, from http://ehstoday.com/safety/management/managing-social-networking-policies-1202/.
9. Erigami (2010) Truwex Online, Web Accessibility Testing Tool: WCAG, Section 508 compliance, Retrieved March 1, 2010, from http://checkwebsite.erigami.com/accessibility.html.
10. Europa, (2009, September 26) Social Networking Sites: Commissioner Reding stresses their economic and societal importance for Europe, Retrieved March 3, 2010, from http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/08/587.
11. Fernandez, P. (2009) Balancing outreach and privacy in Facebook: five guiding decision points, *Library Hi Tech News*, Number 3/4, 10-12.
12. Gunasekara, G. & Toy, A. (2008) MySpace" or Public Space: The Relevance of Data Protection Laws to Online Social Networking, *New Zealand Universities Law Review*, December 2008, Volume 23 (Issue 2), 191-214
13. IBM (2010) Rational Policy Tester Privacy Edition, IBM Corporation. Retrieved March 1, 2010, from http://www-01.ibm.com/software/awdtools/tester/policy/privacy/
14. Hinduja, S. (2004) Theory and Policy in Online Privacy, *Knowledge, Technology & Policy*, Spring 2004, Volume 17 (Issue 1), 38-58.
15. Hooper, T. & Vos, M. (2009) Establishing business integrity in an online environment: An examination of New Zealand web site privacy notices, *Online Information Review*, Volume 33 (Issue 2), 343-361.
16. Hung, H. & Wong, Y. (2009) Information transparency and digital privacy protection: are they mutually exclusive in the provision of e-services?, *Journal of Services Marketing*, Volume 23 (Issue 3), 154-164.
17. Johnson-Page, G. & Thatcher, R. (2001) B2C data privacy policies: current trends, *Management Decision*, Volume 39 (Issue 4), 262-271.
18. Levin, A. & Abril, P. (2009) Two Notions of Privacy Online, *Vanderbilt Journal of Entertainment & Technology Law*, Volume 11, 1001-1051.
19. Liu, C. & Arnett, K. (2002) An Examination of Privacy Policies in Fortune 500 Web Sites, *Mid-American Journal of Business*. Spring 2002, Volume 17 (Issue 1), 13-21.
20. McRobb, S. & Rogerson, S. (2004) Are they really listening? an investigation into published online privacy policies at the beginning of the third millennium. *Information Technology & People*, Volume 17 (Issue 4), 442-461.
21. Nielsen Company (2009, March) Global Faces and Networked Places: A Nielsen report on Social

Networking's New Global Footprint, Retrieved March 22, 2010, from http://blog.nielsen.com/nielsenwire/wp-content/uploads/2009/03/nielsen_globalfaces_mar09.pdf.
22. Phillips, D. (2004) Privacy Privacy policy and PETs: The influence of policy regimes on the development and social implications of privacy enhancing technologies, New Media & Society, *Dec 2004; Volume 6 (Issue 6), 691-706.*
23. Preibusch, S., Hoser, B., Gurses, S. & Berendt, B. (2007) Ubiquitous social networks - opportunities and challenges for privacy-aware user modelling, In: *Proceedings of Workshop on Data Mining for User Modeling*, June 2007, Corfu, Greece.
24. Shalhoub, Z. (2006) Trust, privacy and security in electronic business: the case of the CGG countries, *Information Management & Computer Security*, Volume 14 (Issue 3), 270-283.
25. "*Social networks* hide *privacy* policies to stay popular," (2000), *New Scientist*, 203(2719), 4.
26. Turow, J. (2003) Americans and Online Privacy: The System is Broken, Report of the Annenberg Public Policy Center, Retrieved March 8, 2010, from : http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf
27. W3C (2007) Enabling smarter Privacy Tools for the Web, Retrieved March 8, 2010, from http://www.w3.org/P3P/
28. W3C (2010) P3P Validator, W3C.org, Retrieved March 1, 2010, from http://www.w3.org/P3P/validator.html.
29. Wirtz, J., Lwin, M. & Willians, J. (2007) Causes and consequences of consumer online privacy concern, *International Journal of Service Industry Management*, Volume 18 (Issue 4), 326-348.
30. Wu, M. (2008) How Accessible is Government of Saskatchewan Website, *Presentation to CMPT 480 Accessible Computing*. Retrieved March 1, 2010, from http://www.cs.usask.ca/classes/480/t2/Shawn%20presentation.ppt.