Do I Know What You Can See? Social Networking Sites and Privacy Management

Regina Collins
Information Systems, New Jersey Institute of Technology, Newark, NJ, United States., rsb24@njit.edu

Catherine Dwyer
Information Systems, Pace University, New York, NY, United States., cdwyer@pace.edu

Starr Hiltz
Information Systems, New Jersey Institute of Technology, Newark, NJ, United States., roxanne.hiltz@njit.edu

Harshada Shrivastav
Information Systems, New Jersey Institute of Technology, Newark, NJ, United States., hps9@njit.edu

Do I Know What You Can See? Social Networking Sites and Privacy Management

Regina Collins
New Jersey Institute of Technology
rsb24@njit.edu

Catherine Dwyer
Pace University
cdwyer@pace.edu

S. Roxanne Hiltz
New Jersey Institute of Technology
roxanne.hiltz@gmail.com

Harshada Shrivastav
New Jersey Institute of Technology
hps9@njit.edu

ABSTRACT

Social networking sites invite users to share personal information with their connections, allowing individuals to easily maintain their social capital. The sharing of personal information on social networking sites can bring positive outcomes; however, it can also lead to issues such as identity theft and cyberbullying. This research examines the privacy practices of Facebook users, capturing not only their usage and perceptions of Facebook's privacy management capabilities but also adaptations such as self-censorship of shared information. Data from the current study are compared with data collected in 2007; results suggest that Facebook users today are even more actively engaged in privacy management, are less likely to accept friend requests from unknown entities, and are more proactive in their responses to privacy incidents.

Keywords

Online privacy management, social software, social networking site.

INTRODUCTION

Social network sites (SNS) enable individuals to create profiles that describe themselves and their interests, designate their friends or social connections, and navigate those connections to explore additional connections (boyd and Ellison 2007). To facilitate this connection building, social networking sites store personal data that, if shared properly, can enhance social exchanges and simplify the building or maintenance of critical social capital. That same data, however, could be used for, at the least, unsolicited advertising or social contact and, at the worst, identity theft and cyberbullying. Facebook, a dominant force amongst social networking sites, has implemented privacy management tools to give its 800 million plus users control over the visibility and accessibility of their personal data. Yet users have expressed frustration and concern over these measures and their implementation and, in November of 2011, Facebook reached a settlement with the United States Federal Trade Commission based on charges that Facebook "deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public" (ftc.gov 2011).

Sharing personal information is a central concept in social networking sites, as evidenced by Facebook's homepage message of enabling users to "connect and share with the people in your life." Users can choose to share everything from birthdate, home town and relationship status to popular links, photos, and videos. Facebook's privacy controls are intended to allow users to manage who can view their shared information; however, frequent changes to Facebook's privacy settings have often gone unnoticed or have only confounded users' attempts to appropriately manage their privacy. These changes also affect users' perceptions of the efficacy of these privacy measures in actually protecting their privacy and safeguarding their personal information. Particularly in light of Facebook's recent settlement with the United States Federal Trade Commission (FTC), the efficacy (both perceived and actual) of Facebook's privacy settings can provide a foundation for researchers and designers of privacy management controls in any type of computer-mediated communication system.

This paper reports results of the third in a series of studies of Facebook users, based on different university-based snowball samples. These results are a continuation of the study of privacy management strategies for members of SNS that began in 2006. Prior studies include a quantitative study comparing privacy management strategies between Facebook and MySpace members (Dwyer, Hiltz, and Passerini 2007), an examination of privacy management strategies of Facebook and MySpace members from the same community (Dwyer 2008), and an examination of privacy management strategies for a SNS based in Europe, StudiVZ (Dwyer, Hiltz, Poole, Gussner, Hennig, Osswald, Schleissberger, and Warth 2010). With this study, we

repeat many of the same measures of privacy management and look for continuities and changes in the strategies members deploy to manage their privacy. Key research questions are:

RQ1: *How has usage of privacy management settings in Facebook changed since 2007?*

RQ2: *What are Facebook members' attitudes towards unknown entities and unsolicited contacts?*

RQ3: *Has there been a change in the number of privacy incidents on Facebook? Have user responses to such incidents changed?*

The following section provides a review of privacy management literature, particularly as it relates to social networking sites. This is followed by a brief description of the research methodology and an analysis of resulting data regarding privacy management, privacy incidents and attitudes towards data sharing. The final section of this paper discusses the study's limitations and plans for future research.

RELATED LITERATURE

Research regarding privacy concerns and their impact on the employment of SNS privacy management tools has resulted in inconsistent findings. Acquisti and Gross (2006) examined the relationship between reported privacy concerns and actual behavior of college students; their findings indicated that even students with high levels of privacy concerns still joined SNS and disclosed information such as their home addresses or class schedules. Similar results were reported by Awad and Krishnan (2006) in their description of the "Personalization Privacy Paradox". Stutzman, Capra and Thompson (2011) examined the relationship between disclosure and privacy concerns, finding that users who had personalized their privacy settings were more willing to share information about themselves, while users who had reviewed a site's privacy policies were less likely to disclose personal information. Dwyer, Hiltz and Passerini (2007) examined users' trust in both the SNS and its members, comparing users of Facebook and MySpace. They found that Facebook members reported a higher level of trust in the site and its commitment to protect their information than MySpace members and also reported a lower level of distrust of users' self-presentations.

DeSanctis and Poole (1994) proposed the Adaptive Structuration Theory (AST) to examine the process of technology appropriation by individuals in a social setting. AST was originally developed to examine group interaction in group decision support systems, focusing particularly on appropriation moves that specified how technology was appropriated by the individuals using it as well as how these appropriated technologies subsequently impacted the organization in which they were embedded. "AST builds on structuration theory and explains use in terms of technology structures and their interaction with social structures that emerge as people use the technology" (Dwyer 2008). An examination of AST appropriation moves and their applicability to SNS privacy management yielded a theoretically-based framework of five moves tested and validated by Dwyer et al. (2010).

Other researchers have found that users of social networking sites were not always aware of the privacy setting default values or even of the structures allowing them to modify privacy settings. Gross and Acquisti (2005) conducted research on Carnegie Mellon University's Facebook student population, determining that 15.7% of female students and 21.2% of male students had disclosed sufficient personal information to make themselves susceptible to stalking in real life. A similar study by Jones and Soltren (2005) collected data from four institutions; within one week, they were able to mine data from tens of thousands of student profiles. This same data can be mined by prospective employers (Kluemper and Rosen 2009; Rosenblum 2007) as a way to gather personal information about a job candidate that cannot be collected through the interview process.

More recently, Madejski, Johnson and Bellovin (2011) conducted a study of Columbia University students using Facebook, comparing students' perceptions of the visibility of their personal information with the actual visibility of that information. Privacy violations were categorized into: 1) hide violations in which information that the students intended to hide was visible; and 2) show violations in which information the student wanted to share was not visible. Research results indicated that 93.8% of students' had visible information that they thought was hidden; 84.6% of students' had hidden information that they thought was visible. Other research regarding privacy incidents found that, of the 15% of users who reported some form of privacy incident while using a social networking site, only 50% reported subsequently reviewing or modifying their privacy settings (Dwyer and Hiltz 2008).

RESEARCH METHODOLOGY

To develop a research framework for examining the use of privacy management measures, (Dwyer et al. 2010) applied DeSanctis and Poole's (1994) Adaptive Structuration Theory (AST) to research the appropriation of privacy management

tools in SNS. The result was a theoretically-based framework for recognizing and measuring the appropriation of these structures; the scales in this framework were tested and validated through surveys of Facebook, MySpace, and StudiVZ users (Dwyer et al. 2010).

In light of Facebook's frequent privacy setting changes and its recent settlement with the FTC regarding violations of its privacy policies, this study focuses on re-examining the AST appropriation moves validated by (Dwyer et al. 2010, based on data collected in 2007) to provide a comparison of the appropriation of privacy management practices in 2007 and 2011. An online survey was developed that included the factor measures analyzed in the previous study, along with questions specifically addressing privacy incidents and user responses to such incidents (i.e. reviewing and/or changing their privacy settings) (Dwyer and Hiltz 2008).

In November, 2011, the online survey was made available for approximately one month; participants were recruited through snowball sampling. An initial invitation to the survey was distributed by two students and a professor from a northeastern public university in the U.S. (The randomly generated sample from the 2007 survey was also initiated at this same university). Invitations to the 2011 survey were also distributed at universities in Canada and India. These invitations were distributed through e-mail and postings on Facebook and other social media sites. The invitation requested not only the person's participation but also sharing of the invitation with others. A $50 gift certificate was offered for one randomly drawn respondent out of each respondent cohort of 100. A total of 149 respondents accessed the survey.

Privacy Management Appropriation Measures

The (Dwyer et al. 2010) study applied Adaptive Structuration Theory (AST) to social networking sites to develop reliable measures of online privacy management. Having developed such measures and tested them with users of three different SNS, Dwyer et al. established a framework through which researchers could compare outcomes for various social networking sites. In this study, changes in perceptions regarding Facebook privacy management are being evaluated based on the results collected in 2007 (reported in the 2010 paper) with results collected four years later in late 2011.

Dwyer et al. selected five appropriation moves from DeSanctis and Poole's (1994) original definition of AST to apply to privacy management on social networking sites. The Use appropriation move measures the degree to which users report actually using the privacy settings available in the site. The Familiar appropriation move ascertains the degree to which users feel they are familiar with privacy management functionality. The Restricted Scope appropriation move captures to what extent users are willing to accept or initiate new relationships online. The Rejection appropriation move explores to what extent users do not actively manage their privacy settings. The final scale proposed by Dwyer et al. (2010) is the Faithfulness scale which was intended to capture whether users felt they were utilizing the privacy management tools as the designers had intended. Distrust measures which were part of the Dwyer et al. 2007 study were included to ascertain the level of distrust users report regarding their interactions with other Facebook members. Two additional measures, labeled Active1 and Active2, were repeated from the 2007 study to capture users' perceptions regarding how actively they manage their privacy settings in Facebook.

Privacy Incidents

Dwyer and Hiltz (2008) propose a re-examination of how privacy management is implemented in social networking sites. To identify issues with existing implementations of privacy settings, the researchers included questions asking users about privacy incidents which had occurred within the last year. This question and the two follow-up questions for those responding in the affirmative (did they subsequently review their privacy settings and did they make any adjustments to their privacy settings) were included in the current study to identify whether privacy incidents had increased or decreased since the original study, and whether affected users had become more or less proactive in their responses to privacy incidents.

RESULTS

In total, 149 potential respondents accessed the 2011 online survey while the 2007 survey yielded 107 potential respondents, although in both cases some participants did not complete portions of the survey. Among those who provided basic demographic information, frequencies and means for gender, age, ethnicity, and academic status are shown in Table 1. Although gender distribution remained similar between the two studies, the distributions of other demographic factors changed between the two respondent samples. The large percentage of Asian respondents in the 2011 cohort is accounted for by the fact that the survey was distributed by a professor at a university in India as well as the largely Asian population of graduate students at the university originating the survey.

Category	Value	Frequency (Percent) or Mean/SD		
		2011	**2007**	**Difference**
Gender	Male	79 (67%)	77 (72%)	$\chi^2 = 0.663$,
	Female	39 (33%)	30 (28%)	p = 0.41
Age		M=28, SD = 10.9	M=23, SD = 5.1	**t = 4.40 p < .0001**
Ethnicity	Caucasian	42 (38%)	51 (49%)	**$\chi^2 = 12.51$, p = .0019**
	Asian	58 (52%)	31 (30%)	
	Other	11 (10%)	22 (21%)	
Academic Status	Undergraduate	38 (38%)	58 (61%)	**$\chi^2 = 16.43$, p = .0003**
	Graduate	57 (57%)	27 (28%)	
	Others (including staff or those not in Academia)	5 (5%)	10 (11%)	

Table 1 Respondent Demographics

Privacy Management Appropriation Measures

The appropriation measures included in this study are based on earlier studies of Facebook privacy management (Dwyer et al. 2007; Dwyer et al. 2010) and are listed in Table 2. (Responses to measures are based on a seven-point Likert-type scale with values ranging from Strongly Disagree (1) to Strongly Agree (7).) As in the (Dwyer et al. 2010) study, factor analysis was conducted on the appropriation measures to ensure that each measure loads on only one factor. As recommended by Hair, Black, Babin, Anderson and Tatham (2006), a Principal Component Analysis was first conducted to determine the number of factors to keep. Five factors were identified, explaining 70.77% of the variance. Subsequently, the factors were rotated using Varimax rotation to achieve a more readily interpretable solution. The factor loadings from previous studies were compared to the current loadings; while some factors remained fairly stable (Distrust, Familiarity and Scope), others factors were not consistent across the two studies; results of the factor analysis will not be reported in this paper. Instead, this paper examines the changes in means of the measures in the four years since the first Facebook privacy survey, shown in Table 2.

		Facebook 2011		**Facebook 2007**		**Difference**	
Meas.	**Statement**	**Mean**	**SD**	**Mean**	**SD**	**t value**	**p val.**
Use1	I have personalized my privacy settings on Facebook.	5.61 n=106	1.78	4.82 n=106	2.06	**-3.00**	**0.0030**
Use2	I have modified the privacy settings for my profile on Facebook.	5.84 n=106	1.68	4.67 n=104	2.19	**-4.33**	**<.0001**
Use3	I have adapted the privacy settings to control who can view my profile on Facebook.	5.48 n=107	1.75	4.26 n=105	2.16	**-4.52**	**<.0001**
Active1	I have changed the default settings for my profile to make it more private.	5.68 n=104	1.67	4.30 n=107	2.18	**-5.17**	**<.0001**
Active2	I have taken time to learn how I can change my settings to protect my privacy.	5.43 n=104	1.85	3.06 n=105	1.89	**-9.19**	**<.0001**
Fam1	When I need to modify my privacy settings for Facebook, I am able to do it.	5.79 n=106	1.63	5.49 n=105	1.41	-1.46	0.1446
Fam2	I am confident that I know how to control who is able to see my profile on Facebook.	5.30 n=107	1.82	4.79 n=106	1.74	**-2.07**	**0.0392**
Fam3	I am comfortable with my ability to adjust my	5.50	1.69	5.19	1.67	-1.34	0.1829

	privacy settings.	n=105		n=107			
Reject1	Adjusting the privacy settings for Facebook is a waste of time.	2.01 n=105	1.42	2.25 n=107	1.42	1.25	0.2144
Reject2	I don't bother to look at the privacy settings for my profile on Facebook.	2.25 n=104	1.77	3.30 n=107	2.11	**3.91**	**0.0001**
Reject3	I don't know what my privacy settings are on Facebook.	2.24 n=106	1.71	3.00 n=107	2.04	**2.96**	**0.0034**
Scope1	I never accept friend requests from people I have not met in person.	5.26 n=107	1.92	4.57 n=107	2.07	**-2.53**	**0.0120**
Scope2	When using Facebook, I ignore contact from people whom I do not already know.	5.67 n=106	1.71	4.63 n=106	1.91	**-4.16**	**<.0001**
Scope3	I don't use Facebook to make contact with people whom I've never heard of.	6.03 n=105	1.48	5.42 n=107	1.95	**-2.56**	**0.0112**
Distrust1	I have been contacted by people whom I did not trust through Facebook.	4.22 n=107	2.17	3.19 n=105	1.84	**-3.74**	**0.0002**
Distrust2	I don't believe most of the information people put on their profiles on Facebook.	4.06 n=105	1.49	3.37 n=107	1.56	**-3.27**	**0.0013**
Distrust3	There are a lot of profiles on Facebook for people who do not seem trustworthy.	5.28 n=106	1.46	4.38 n=106	1.78	**-4.05**	**<.0001**

Table 2 Comparison of Means for Privacy Management Measures

In comparing the data from the 2007 and 2011 studies, the means for the measures reflecting usage of privacy management (Use) and active engagement in privacy management (Active) have increased, suggesting that contemporary users are more actively engaged in monitoring their privacy settings than survey participants from four years ago. In terms of the question asked in the title of this paper, results for Fam2 show that there appears to be a slight increase in users' confidence that they can control who is able to see their profile, but that this level of confidence is not very high. Concurrently, the means for two of the Reject measures (Reject2, Reject3) which capture non-use of privacy management tools decreased, suggesting again that users are making an effort to review and understand their Facebook privacy settings. In combination, the 2011 data are more polarized (stronger agreement with positively coded statements and stronger disagreement with negatively coded statements), suggesting increased participation in privacy management by Facebook users. The increase in means for the Scope measures suggests that current Facebook users are even less interested in initiating new relationships through Facebook, using the site instead to maintain existing relationships. Along with the diminished use of Facebook to create new relationships, there is a significant increase in the Distrust measures. One possible explanation for this is the effect of increased levels of Distrust – respondents do not place much trust in unknown people or their profiles on Facebook. However, because the data samples were drawn from different populations, this might explain some or all of the apparent differences.

Privacy Incidents

Almost half of the 2011 respondents (46.6%) indicated that they experienced an incident that led them to be concerned about privacy while using Facebook during the past year. This indicates a significant change from the Dwyer and Hiltz (2008, based on data collected in 2007) study in which only 15% of respondents indicated experiencing a privacy incident. For those who responded affirmatively, the survey prompted them to indicate if they had reviewed their privacy settings after the incident and if they had made any changes to their privacy settings after the incident. Results are shown in Table 3.

	2011 Facebook		**2007 Facebook**	
Over the past year did you experience any incidents that led you to be concerned about privacy when using [name of SNS]?				
	n	**%**	**n**	**%**
Yes	48	46.6%	16	15.0%

No	55	53.4%	91	85.0%
Total	103		107	
(For those who responded Yes to the first question) Did you review your privacy settings after this incident?				
Yes	38	79.2%	8	50.0%
No	10	20.8%	8	50.0%
Total	48		16	
(For those who responded Yes to the first question) Did you make any adjustments or changes to your privacy settings after this incident?				
Yes	39	81.2%	8	50.0%
No	9	18.8%	8	50.0%
Total	48		16	

Table 3 Comparison of Privacy Incidents and Responses

The 2007 data indicated that only 50% of Facebook users who had experienced a privacy incident reviewed or made changes to their privacy settings afterwards. Again, this differs substantially from the 2011 results in which 81.2% of those who had experienced a privacy incident made subsequent changes to their privacy settings.

Madejski et al. (2011) found that SNS users were most likely to modify past and future privacy settings in instances where non-friends could view information that the respondents wanted to keep private. Of the 65 participants in their study, 35 reported they would take action to hide information they wished to keep private from friends of friends, 36 would take action to hide information from network members, and 47 of 65 respondents would take action to hide information from strangers.

Respondent Comments

The survey invited respondents to provide any additional comments regarding Facebook usage and privacy concerns. Many of these comments fell into one or more of the categories discussed below.

Self-Censorship of Information

Several respondents described a method of self-censorship that assisted in reducing their privacy concerns. These respondents indicated that they avoided posting personal information on Facebook, keeping their information fairly trivial. As one respondent stated, "*I really do not reveal much about my personal life on Facebook, which is partly why I am not very worried about my privacy being invaded*." Another stated, "*I minimize the non-trivial information I put on Facebook.*"

Privacy Settings

Several respondents indicated frustration with Facebook's privacy settings in terms of ease of use, frequent changes, and implementation. One respondent indicated a lack of trust that Facebook's privacy settings are actually effective, saying, "*I am confident that I know how to set my privacy settings, but I am not confident that Facebook has properly implemented the privacy settings…*" Another respondent felt confident regarding profile settings but was unaware that tagged photos could be seen by people other than Facebook friends and friends of friends: *I don't know what I could do to make sure that when I'm tagged that ONLY my friends/friends-of-friends can check these photos out. I am now on a mission to figure this out.*"

Several respondents commented that they found Facebook's privacy settings confusing or burdensome. One respondent stated, "*Their privacy settings are confusing … apparently people on my restricted list can still see information or posts that I do not wish to share with them*." A final example reflected many Facebook users' frustrations with the frequent (and unannounced) privacy changes: "*When Facebook releases an update, it shouldn't have to reset privacy settings to the defaults every time. I feel that this is a ploy that allows third-parties and aggregators to sift through data for the purpose of marketing. If that is the case, I feel that it is immoral.*"

DISCUSSION

The results described in the previous sections suggest that Facebook users are more concerned with maintaining the privacy of their data on Facebook than they were four years ago. In response to RQ1, the changes in means of the Use and Active measures suggest that, in 2011, Facebook members are more actively engaged in reviewing and applying privacy management settings to control the visibility of their personal information than they were in 2007. Possible explanations for this increase include more familiarity with social networking sites or concerns regarding identity theft. However, respondents' comments also suggest that there are general concerns regarding Facebook's implementation of privacy management and its commitment to properly managing users' personal data; one of the eight complaints against Facebook listed in the FTC settlement is that Facebook changed its privacy settings so that information users set as private became publicly visible.

RQ2 examines Facebook users' attitudes towards unknown entities and unsolicited contacts. The increase in means of the Scope measures from 2007 to 2011 suggest that Facebook users are even less likely to accept contact or friend requests from individuals they do not already know, suggesting that Facebook's principle usage is to maintain offline social capital rather than to expand online social capital. A possible explanation for this is suggested by the increasing means of the Distrust measures which capture users' distrust of unknown entities on Facebook.

To respond to RQ3, this study compares privacy incidents in 2011 with those reported in the 2007 survey (Dwyer and Hiltz 2008). Forty-six percent of respondents in the current study reported experiencing some form of privacy incident within the past year; this is an increase of over 30% from Dwyer and Hiltz's reported 15% in 2008. A comparison of the follow-up questions indicates that current Facebook users are more proactive in reviewing and modifying their privacy settings after an incident has occurred (81% in the current study, an increase of over 30% from Dwyer and Hiltz's reported 50% in 2008).

CONCLUSION

Facebook users are concerned about maintaining the privacy of their information online; to achieve this, they are taking an active role in managing their privacy settings on Facebook and also implementing techniques such as self-censorship to ensure that their online privacy is not violated. For those who have experienced some sort of privacy violation, most are now actively reviewing and modifying their settings in an effort to reduce the possibility of future violations. Users have accepted that the burden of maintaining their online information rests squarely on their shoulders. Both the 2011 survey data and the comments of users indicate that substantial numbers of Facebook users feel that they do not know for certain who can see various types of data about them, and that they distrust Facebook in terms of safeguarding their privacy.

Researchers such as Dwyer and Hiltz (2008) have argued that social networking sites can and should do more to protect their users' privacy. Instead of treating privacy management as a task-related system requirement, designers should evaluate privacy management as a non-functional system requirement. At the same time, researchers should continue to explore not only user perceptions and experiences regarding privacy management in social networking sites, but also apply theoretical constructs to design and action research focusing on the "design of IT artifacts for the protection and control of information privacy" (Pavlou, 2011).

Limitations and Future Work

This research reapplies measures from previous studies of Facebook to identify changes in users' perceptions regarding privacy management as well as usage of privacy settings. Respondents for the survey were solicited via snowball sampling and have an oversampling of university students. Snowball sampling was used because it is not possible to obtain a list of Facebook users to serve as a sampling frame. In addition, the sampling frames for the various studies are not comparable. Thus, changes in privacy concerns are confounded with differences in the sampling frames. Follow-up research should seek to solicit input from other cohorts of Facebook users to identify any discrepancies that may arise from a non-representative sample.

Results of the research are presented based on univariate analysis comparing data from two distinct respondent samples. Future research will include model construction and path analysis of the collected data.

REFERENCES

1. Acquisti, A. and Gross, R. (2006) Imagined Communities: Awareness, Information Sharing and Privacy on The Facebook, *Paper presented at the 6th Workshop on Privacy Enhancing Technologies*, Cambridge, UK.

2. Awad, N.F. and Krishnan, M.S. (2006) The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willigness to be Profiled Online for Personalization. Management Information Systems Quarterly 30, 1, 13-
3. boyd, d.m., Ellison, N.B. (2007) Social Network Sites: Definition, History, and Scholarship, *Journal of Computer-Mediated Communication* 13, 1, 210-230.
4. Dennis, A., Wixom, B. and Vendenberg, R. (2001) Understanding Fit and Appropriation Effects in Group Support Systems via Meta-Analysis, *MIS Quarterly* 25, 167-193.
5. DeSanctis, G. and Poole, M.S. (1994) Capturing the Complexity in Advanced Technology Use: Adaptive Structuration Theory, *Organization Science* 5, 2, 121-147.
6. Dwyer, C. (2008) *Appropriation of Privacy Management Within Social Networking Sites*. Newark, NJ: New Jersey Institute of Technology.
7. Dwyer, C. and Hiltz, S. R. (2008) Designing Privacy Into Online Communities, *Proceedings of Internet Research 9.0*, October 15 – 28, Copenhagen, Denmark.
8. Dwyer, C., Hiltz, S. R., and Passerini, K. (2007) Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace, *Proceedings of Americas Conference on Information Systems (AMCIS)*.
9. Dwyer, C., Hiltz, S. R., Poole, M. S., Gussner, J., Hennig, F., Osswald, S., Schleissberger, S. and Warth, B. (2010) Developing Reliable Measures of Privacy Management Within Social Networking Sites, *Proceedings of the 43rd Annual Hawaii International Conference on System Sciences (HICSS)*, January 5-8, Honolulu, HI, USA.
10. Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises. www.ftc.gov, Federal Trade Commission, n.d. Web. Accessed 11 Jan. 2012.
11. Gross, R. and Acquisti, A. (2005) Information revelation and privacy in online social networks. *2005 ACM Workshop on Privacy in the Electronic Society*, ACM.
12. Hair, J., Black, W., Babin, B., Anderson, R. and Tatham, R. (2006) *Multivariate Data Analysis*. Upper Saddle River: Prentice Hall.
13. Hiltz, S. R. and Turoff, M. (1993) *The Network Nation: Human Communication via Computer* (Revised edition (from 1978) ed.). Cambridge: MIT Press.
14. Jones, H. and Soltren, J. H. (2005) Facebook: Threats to Privacy. http://www-swiss.ai.mit.edu/6805/student-papers/fall05-papers/facebook.pdf.
15. Kluemper, D.H. and Rosen, P.A. (2009) Future employment selection methods: evaluating social networking web sites, *Journal of Managerial Psychology* 24, 6, 567-580.
16. Lipford, H. R., Besmer, A. and Watson, J. (2008) Understanding Privacy Settings in Facebook with an Audience View. *First Conference on Usability, Psychology, and Security*, USENIX Association.
17. Madejski, M., Johnson, M. and Bellovin, S. (2011) *The Failure of Online Social Network Privacy Settings*, Technical Report CUCS-010-11, Columbia University, February.
18. Pavlou, P. (2011) State of the Information Privacy Literature: Where Are We Now and Where Should We Go?, *MIS Quarterly* 35, 4, 977-988.
19. Rosenblum, D. (2007) What Anyone Can Know: The Privacy Risks of Social Networking Sites, *IEEE Security and Privacy* 5, 3, 40-49.
20. Stutzman, F., Capra, R. and Thompson, J. (2011) Factors Mediating Disclosure in Social Network Sites, *Computers in Human Behavior 27*, 590-598.