Security and privacy issues: Does association has role to play?

Mr. K Sanal Nair
Data Analyst, Mount Litera Zee School, Bangalore, +91 725936185, Sanalnair1@gmail.com

Abstract

Social Networking Sites (SNS) users are concerned of their Internet privacy and security and intend to achieve total anonymity while communicating online. In order to keep their information private, they need to be careful on what they submit and look at online. Hence it becomes important to study these security and privacy issues for the better management of future internet search and access. We attempt to study the behavior of users towards security and privacy issues on social networking sites across various demographics selected for the study. 200 questionnaires were distributed among the various majors in the five major cities of Rajasthan and of which only 128 responses were complete in all respects and hence were considered for the study. Cronbach alpha values were found to be 0.78 indicating the data to be reliable. F-test ANNOVA was used to find out the significance of association/ non association between the variables selected for the study. It was found that users of SNS were fearful about photos and other articles being downloaded , about information displayed being inappropriately used by others about intellectual rights being infringed, copied or abused by others, about identity theft, profiling or phishing and a significant concern that the SNS provider might divulge information to other parties without ones' explicit consent. Different demographics have a different impact on the perception towards security and privacy issues. The concern towards who one was talking to when online was less but in the other cases the concern was significantly high.

Key words: Privacy, Personal information, Security, Social Networking Sites.

ISSN 2348–0661 Print

Introduction

Social Networking Sites (SNS) have become very popular during the past few years, as they allow users to both express their individuality and meet people with similar interests. It has been witnessed that there is a dramatic rise in the popularity of online social networking services, with several Social Network Sites (SNSs) such as Myspace, Facebook, Blogger, You Tube, Yahoo! Groups etc. which are now among the most visited websites around the world. One serious issue while communicating online is issue of privacy of communication and the security of the ones concerned. Security and privacy related to social networking sites are fundamentally behavioral issues, not technology issues. People who provide private, sensitive or confidential information about themselves or other people, whether willingly or unwillingly, pose a higher risk to themselves and others (Pelgrin, 2010). Presently the volume of personal information available on social networking sites is increasing and has attracted malicious people who seek to exploit this information. However, since such forums are relatively easy to access and the users are often not aware of the size and the nature of the audience accessing their profiles, they often reveal more information which is not appropriate to a public forum. As a result, such commercial and social site may often generate a number of privacy and security related threats for the members (Hasib, 2008). Nonetheless, there are also many potential threats to privacy associated with these SNS such as identity theft and disclosure of sensitive information. However, many users still are not aware of these threats and the privacy settings provided by SNS are not flexible enough to protect user data (Ai Ho, 2009). One should ensure that any computer one uses to connect to a social media site has proper security measures in place. One should use and maintain anti-virus software and keep application system up-to-date. Many applications embedded within social networking sites require you to share your information when you use them. Hackers use these sites to distribute their malware. Use strong and unique passwords. Using the same password on all accounts increases the vulnerability of these accounts if one becomes compromised. Do not assume privacy on a social networking site. For both business and personal use, confidential information should not be shared. Users should only post information which are comfortable disclosing to a complete stranger. They should configure privacy settings to allow only those people who are trusted to have access to the information one posts and should also restrict the ability for others to post information to one's page. If a site's privacy policy is fake or does not properly protect one's information, he shouldn't use the site. As Security and privacy issues on social networking sites are related to behavioral issues and not technology issues. It has become very important to study the behavior of people towards these issues. The variables identified to study privacy and security issues on social networking sites were as follows:

- Concern that the information displayed specifically to someone may be inappropriately forwarded to others.
- Concern that the photos shown in one's profile may be downloaded and transmitted by others.

ISSN 2348–0661 Print

- Concern that the people you one only know online are not who they say they are.
- Concern that other people might reveal ones real identity and personal information online without their consent.
- Concern that your intellectual properties might be copied or abused by others (For example: articles, photos and ideas).
- Concern about online identity theft, profiling or phishing.
- Concern that the SNS provider might divulge ones information to other parties without his/her explicit consent.

Review of literature

(Barnes, 2006) discussed the uproar over privacy issues in social networks by describing a privacy paradox; private versus public space; and, social networking privacy issues. The discussion finally proposed privacy solutions and steps that could be taken to help resolve the privacy paradox. **(Shin, 2010)** revealed that perceived security moderates the effect of perceived privacy on trust. Based on the results of this study, practical implications for marketing strategies in SNS markets and theoretical implications were recommended accordingly. **(Matthew M. Lucas, 2008)** aimed to mitigate the risk by presenting a new architecture for protecting information published through the social networking website, Facebook, through encryption. Their architecture made a trade-off between security and usability in the interests of minimally affecting users' workflow and maintaining universal accessibility. While active attacks by Facebook could compromise users' privacy, their architecture dramatically raised the cost of such potential compromises and, importantly, placed them within a framework for legal privacy protection because they would violate a user's reasonable expectation of privacy. They built a prototype Facebook application implementing there architecture, addressing some of the limitations of the Facebook platform through proxy cryptography. **(Ralph Gross, 2005)** analyzed the online behavior of more than 4,000 Carnegie Mellon University students who joined a popular social networking site catering to colleges. They evaluated the amount of information they disclosed and studied their usage of the site's privacy settings. They highlighted potential attacks on various aspects of their privacy, and showed that only a minimal percentage of users changed the highly permeable privacy preferences. **(Gartrell & Han, 2009)** presented several of their privacy and security issues, along with their design and implementation of solutions for these issues. Their work allows location-based services to query local mobile devices for users' social network information, without disclosing user identity or compromising users' privacy and security. They contended that it is important that such solutions be accepted as mobile social networks continue to grow exponentially. **(Molva & Strufe, 2009)** pointed out that centralized architecture of existing on-line social networks as the key privacy issue and suggested a solution that aimed at avoiding any centralized control. Their solution was an on-line

ISSN 2348–0661 Print

social network based on peer-to-peer architecture. Privacy in basic data access and exchange operations within the social network was achieved with a simple anonymization technique based on multi-hop routing among nodes that trust each other in the social network. Similarly cooperation among peer nodes were enforced based on hop-by-hop trust relationships derived from the social network. **(Carlos Flavián, 2006)** revealed that an individual's loyalty to a web site was closely linked to the levels of trust. Thus, the development of trust not only affected the intention to buy, as shown by previous researchers, but it also directly affects the effective purchasing behavior, in terms of preference, cost and frequency of visits, and therefore, the level of profitability provided by each consumer. In addition, they analyzed that trust in the internet was particularly influenced by the security perceived by consumers regarding the handling of their private data. **(Alessandro Acquisti, 2006)** found that an individual's privacy concerns were only a weak predictor of his membership to the network. Also privacy concerned individuals joined the network and revealed great amounts of personal information. Some manage their privacy concerns by trusting their ability to control the information they provide and the external access to it. However, they also found evidence of members' misconceptions about the online community's actual size and composition, and about the visibility of members' profiles. **(Xie & Hengartner, 2009)** proposed FaceCloak, an architecture that protects user privacy on a social networking site by shielding a user's personal information from the site and from other users that were not explicitly authorized by the user. At the same time, FaceCloak seamlessly maintained usability of the site's services. FaceCloak achieved these goals by providing fake information to the social networking site and by storing sensitive information in encrypted form on a separate server. **(Cutillo & Strufe, 2009)** suggested a new approach to tackle these security and privacy problems with a special emphasis on the privacy of users with respect to the application provider in addition to defense against intruders or malicious users. In order to ensure users' privacy in the face of potential privacy violations by the provider, they suggested approaches that adopt a decentralized architecture relying on cooperation among a number of independent parties that were also the users of the online social network application. The second strong point of the suggested approach was to capitalize on the trust relationships that were part of social networks in real life in order to cope with the problem of building trusted and privacy- preserving mechanisms as a part of the online application. **(Amin Tootoonchian, 2009)** presented Lockr, a system that improved the privacy of centralized and decentralized online content sharing systems. Lockr offered three significant privacy benefits to OSN users. First, it separated social networking content from all other functionalities that OSNs provide. This decoupling let users control their own social information: they could decide which OSN provider should store it, which third parties should have access to it, or they could even choose to manage it themselves. Such flexibility better accommodated OSN users' privacy needs and preferences. Second, Lockr ensured that digitally signed social relationships need to access social data and cannot be re-used by the OSN for unintended purposes. This feature drastically reduced the value to others of social content that users entrusted to OSN providers. Finally, Lockr enabled message encryption

ISSN 2348–0661 Print

using a social relationship key. This key let two strangers with a common friend verify their relationship without exposing it to others, a common privacy threat when sharing data in a decentralized scenario. **(Aimeur & Ho, 2010)** highlighted some privacy issues raised by the growing development of SNS and identified clearly three privacy risks. While it may seemed a priority that privacy and SNS were two antagonist concepts, they also identified some privacy criteria that SNS could fulfill in order to be more respectful of the privacy of their users. Finally, they introduced the concept of a Privacy-enhanced Social Networking Site (PSNS) and described Privacy Watch, their first implementation of a PSNS. **(Katherine Strater, 2008)** expanded upon previous research on users' under-utilization of available privacy options by examining users' current strategies for maintaining their privacy, and where those strategies failed, on the online social network site Facebook. The results demonstrated the need for mechanisms that provide awareness of the privacy impact of users' daily interactions. **(Kevin Lewis, 2008)** studied the preference for privacy itself as there unit of analysis, and analyzed the factors that were predictive of a student having a private versus public profile. Drawing upon a new social network dataset based on Facebook, they argued that privacy behavior was an upshot of both social influences and personal incentives. Students were more likely to have a private profile if their friends and roommates had them; women were more likely to have private profiles than men; and having a private profile was associated with a higher level of online activity. Finally, students who have private versus public profiles were characterized by a unique set of cultural preferences—of which the "taste for privacy" may be only a small but integral part. **(Alyson L. Young, 2009)** studied the strategies students had developed to protect themselves against privacy threats. The results showed that personal network size was positively associated with information revelation. No association was found between concern about unwanted audiences and information revelation and finally, students' Internet privacy concerns and information revelation were negatively associated. The privacy protection strategies employed most often were the exclusion of personal information, the use of private email messages, and altering the default privacy settings. Based on their findings, they proposed a model of information revelation and drew conclusions for theories of identity expression. **(Williams, 2010)** surveyed the research literature, in order to provide a current snapshot of privacy and security safeguards for social network websites. They described some of the unique features of the health care space, and recommend directions for future research in this relatively new area.

Research gap

After having an extensive review of literature, it was observed that though there was a vast literature on social networking sites and a number of studies have been done to study the behavior of the users on SNS none of them have tried to study the perception of users towards security and privacy issues on social networking sites, what do they perceive about the security

ISSN 2348–0661 Print

and privacy of their information and communication the kind of information they share, their perception regarding and theft of data or data leakage etc.

Objective of the study

To study the behavior of users towards security and privacy issues on social networking sites across various demographics selected for the study.

Hypothesis framed for the study

H_{01}	There is no significant association between the occupation of the users and the perception towards the security and privacy issues on SNS.
H_{02}	There is no significant association between the reason for using SNS and the perception towards the security and privacy issues on SNS.
H_{03}	There is no significant association between the length of association with SNS and the perception towards the security and privacy issues on SNS.
H_{04}	There is no significant association between the time spent on SNS and the perception towards the security and privacy issues on SNS.

Research methodology

The study used the survey method to approach the respondents through a pre-tested and well structured questionnaire. Only those respondents were chosen who had been using SNS for the past 6 months. The framework was developed using the variables identified during literature review. The questionnaire consisted of respondents' demographic features and the variables related to security and privacy issues. 200 questionnaires were distributed among the various majors in the five major cities of Rajasthan (Jaipur, Jodhpur, Udaipur, Kota and Ajmer) and only 128 responses were complete in all respects (response rate of 64.5%) and hence were considered for the study. Cronbach values were found to be 0.78 indicating the data to be reliable. F-test ANNOVA was used to find out the significance of association/ non association between the variables selected for the study.

Data analysis and Interpretation

Demographic profile (Table 1)

		Frequency	Percent
Gender	Male	83	64.8
	Female	45	35.2

ISSN 2348–0661 Print

	Total	128	100.0
Age	< 15 years	5	3.9
	16-25 years	88	68.8
	26-35 years	27	21.1
	36-50 years	8	6.3
	Total	128	100.0
Educational Qualification	High school	5	3.9
	Intermediate	6	4.7
	Graduation	46	35.9
	Post graduation & above	66	51.6
	Others	5	3.9
	Total	128	100.0
Occupation	Student	81	63.3
	Service(Govt. Sector)	6	4.7
	Service (private)	19	14.8
	Professional	15	11.7
	Business	7	5.5
	Total	128	100.0
Why do you use Social networking sites	Fun & entertainment	53	41.4
	Making new relations	22	17.2
	Social purposes & marketing	50	39.1
	Others	3	2.3
	Total	128	100.0
Length of association with Social networking sites	< 1 year	5	3.9
	2-3 years	37	28.9
	4-5 years	46	35.9
	> 5 years	40	31.3
	Total	128	100.0
Time spent on Social networking sites	Constantly online	22	17.2
	Several times in a day	40	31.3
	Daily	36	28.1

ISSN 2348–0661 Print

	Weekly	30	23.4
	Total	128	100.0

Interpretation

Most of the respondents were male (64.8%) , within the age group of 16-25 years(68.8%), majority of them were pursuing post-graduation and above (51.6%) or graduation (35.9%) , majority of the social networking sites users were students (63.3%) followed by employees of private sector (14.8%) , majority of them use social networking sites for fun and entertainment (41.4%) or social purpose and marketing (39.1%), majority of them (35.9%) have been associated with the social networking sites for a period of 4-5 years and used to surf several times in a day (31.3%) . The above also shows that SNS are mostly used by the youth between the age group of 16-35 years graduates and post graduates students were the most popular users. SNS is most commonly used for fun and entertainment and making new relations, social purpose and marketing and finally SNS are very popular since the past 5 years.

Descriptive statistics (Table 2)

	Mean	**Std. Deviation**
Concern that the information displayed specifically to someone may be inappropriately forwarded to others.	3.12	.838
Concern that the photos shown in one's profile may be downloaded and transmitted by others.	3.48	1.035
Concern that the people you one only know online are not who they say they are.	3.29	1.102
Concern that other people might reveal ones real identity and personal information online without their consent.	3.30	1.105
Concern that your intellectual properties might be copied or abused by others (For example: articles, photos and ideas).	3.40	1.193
Concern about online identity theft, profiling or phishing.	3.44	1.041
Concern that the SNS provider might divulge ones information to other parties without his/her explicit	3.33	1.036

ISSN 2348–0661 Print

consent.		

Interpretation

From the above it was found that the mean of responses was highest with respect to their concern towards the photo shown in their profile may be downloaded and transmitted by others and their intellectual properties be copied or abused by others (For example: articles, photos and ideas). Though users were fearful of the photo and other activities being downloaded, they were motivated to share such information.

The standard deviation was highest in case that the respondents are concerned about their intellectual properties might be copied or abused by others (For example: articles, photos and ideas) and that other people might reveal your real identity and personal information online without your consent. Respondents also varied in their fear that their intellectual property might be copied or abused by others.

Association between demographics and security and privacy issues.

H_{01}: There is no significant association between the occupation of the users and the perception towards the security and privacy issues on SNS.

ANNOVA (Table 3)

		Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Concern that the information displayed specifically to someone may be inappropriately forwarded to others.	Between Groups	19.672	4	4.918	8.695	.000
	Within Groups	69.570	123	.566		
	Total	89.242	127			
Concern that the photos shown in ones' profile may be downloaded and transmitted by others	Between Groups	5.843	4	1.461	1.381	.244
	Within Groups	130.087	123	1.058		
	Total	135.930	127			
Concern that the people you one only know online are not who	Between Groups	8.359	4	2.090	1.761	.141
	Within Groups	145.946	123	1.187		

they say they are.	Total	154.305	127			
Concern that other people might reveal ones real identity and personal information online without their consent.	Between Groups	6.567	4	1.642	1.359	.252
	Within Groups	148.550	123	1.208		
	Total	155.117	127			
Concern that your intellectual properties might be copied or abused by others (For example: articles, photos and ideas).	Between Groups	22.228	4	5.557	4.314	.003
	Within Groups	158.451	123	1.288		
	Total	180.680	127			
Concern about online identity theft, profiling or phishing.	Between Groups	11.911	4	2.978	2.916	.024
	Within Groups	125.589	123	1.021		
	Total	137.500	127			
Concern that the SNS provider might divulge ones information to other parties without his/her explicit consent.	Between Groups	21.503	4	5.376	5.764	.000
	Within Groups	114.716	123	.933		
	Total	136.219	127			

Interpretation

The null hypothesis was accepted in case of concern that the photos shown in ones' profile may be downloaded and transmitted by others, that the people known online were not who they say they are and that other people might reveal the real identity and personal information online without his consent implying that there is no significant association. In all other cases the null hypothesis was rejected indicating a significant influence of the occupation of the users on the perception towards the security and privacy issues relating to SNS.

H_{02}: There is no significant association between the reason for using SNS and the perception towards the security and privacy issues on SNS.

ANNOVA (Table 4)

		Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Concern that the information displayed specifically to someone may be inappropriately forwarded to others.	Between Groups	12.430	3	4.143	6.689	.000
	Within Groups	76.812	124	.619		
	Total	89.242	127			

Concern that the photos shown in ones' profile may be downloaded and transmitted by others	Between Groups	24.380	3	8.127	9.034	.000
	Within Groups	111.549	124	.900		
	Total	135.930	127			
Concern that the people you one only know online are not who they say they are.	Between Groups	9.272	3	3.091	2.643	.052
	Within Groups	145.032	124	1.170		
	Total	154.305	127			
Concern that other people might reveal ones real identity and personal information online without their consent.	Between Groups	14.442	3	4.814	4.244	.007
	Within Groups	140.675	124	1.134		
	Total	155.117	127			
Concern that your intellectual properties might be copied or abused by others (For example: articles, photos and ideas).	Between Groups	19.616	3	6.539	5.034	.003
	Within Groups	161.063	124	1.299		
	Total	180.680	127			
Concern about online identity theft, profiling or phishing.	Between Groups	12.957	3	4.319	4.300	.006
	Within Groups	124.543	124	1.004		
	Total	137.500	127			
Concern that the SNS provider might divulge ones information to other parties without his/her explicit consent.	Between Groups	26.353	3	8.784	9.914	.000
	Within Groups	109.866	124	.886		
	Total	136.219	127			

Interpretation

The null hypothesis was accepted in case of concern that the people known online were not those who they say they were implying no significant association. In all other cases the null hypothesis was rejected indicating a significant influence of the reason for using SNS on the perception towards the security and privacy issues on SNS.

Reason for using SNS

H_{03}: There is no significant association between the length of association with SNS and the perception towards the security and privacy issues on SNS.

ANNOVA (Table 5)

	Sum of	**df**	**Mean**	**F**	**Sig.**

ISSN 2348–0661 Print

		Squares		Square		
Concern that the information displayed specifically to someone may be inappropriately forwarded to others.	Between Groups	1.886	3	.629	.892	.447
	Within Groups	87.357	124	.704		
	Total	89.242	127			
Concern that the photos shown in ones' profile may be downloaded and transmitted by others	Between Groups	11.231	3	3.744	3.723	.013
	Within Groups	124.699	124	1.006		
	Total	135.930	127			
Concern that the people you one only know online are not who they say they are.	Between Groups	7.879	3	2.626	2.224	.089
	Within Groups	146.425	124	1.181		
	Total	154.305	127			
Concern that other people might reveal ones real identity and personal information online without their consent.	Between Groups	7.635	3	2.545	2.140	.099
	Within Groups	147.482	124	1.189		
	Total	155.117	127			
Concern that your intellectual properties might be copied or abused by others (For ex.-articles, photos and ideas).	Between Groups	35.724	3	11.908	10.187	.000
	Within Groups	144.955	124	1.169		
	Total	180.680	127			
Concern about online identity theft, profiling or phishing.	Between Groups	7.698	3	2.566	2.451	.067
	Within Groups	129.802	124	1.047		
	Total	137.500	127			
Concern that the SNS provider might divulge ones information to other parties without his/her explicit consent.	Between Groups	10.532	3	3.511	3.463	.018
	Within Groups	125.687	124	1.014		
	Total	136.219	127			

Interpretation

The null hypothesis was rejected in case of concerned that the photos shown in ones' profile may be downloaded and transmitted by others, that the intellectual properties might be copied or abused by others (For example: articles, photos and ideas) and that the SNS provider might divulge information to other parties without explicit consent implying that there is a significant influence. In all the other cases the null hypothesis was accepted indicating no significant association between the length of association with SNS and the perception towards the security and privacy issues on SNS.

ISSN 2348–0661 Print

H_{04}: There is no significant association between the time spent on SNS and the perception towards the security and privacy issues on SNS.

ANNOVA (Table 6)

		Sum of Squares	df	Mean Square	F	Sig.
You are concerned that the information you displayed specifically to someone may be inappropriately forwarded to others	Between Groups	1.310	3	.437	.616	.606
	Within Groups	87.932	124	.709		
	Total	89.242	127			
You are concerned that the photos shown in your profile may be downloaded and transmitted by others	Between Groups	3.456	3	1.152	1.078	.361
	Within Groups	132.474	124	1.068		
	Total	135.930	127			
You are concerned that the people you only know online are not who they say they are	Between Groups	30.639	3	10.213	10.241	.000
	Within Groups	123.666	124	.997		
	Total	154.305	127			
You are concerned that other people might reveal your real identity and personal information online without your consent	Between Groups	32.387	3	10.796	10.908	.000
	Within Groups	122.730	124	.990		
	Total	155.117	127			
You are concerned that your intellectual properties might be copied or abused by others (For example: articles, photos and ideas)	Between Groups	15.023	3	5.008	3.748	.013
	Within Groups	165.657	124	1.336		
	Total	180.680	127			
You are concerned about online identity theft, profiling or phishing	Between Groups	18.611	3	6.204	6.470	.000
	Within Groups	118.889	124	.959		
	Total	137.500	127			
Are you concerned that the SNS provider might divulge your information to other parties without your explicit consent	Between Groups	20.733	3	6.911	7.420	.000
	Within Groups	115.486	124	.931		
	Total	136.219	127			

Interpretation

The null hypothesis was accepted in case of concern that the information displayed specifically to someone may be inappropriately forwarded to others and that the photos shown in the profile may be downloaded and transmitted by others implying that there is no significant association. In

all other cases the null hypothesis was rejected indicating a significant association between the time spent on SNS and the perception towards the security and privacy issues on SNS.

Conclusions

Security and privacy issues are the most important of the concerns relating to security and privacy issues. The demographics of the respondents have a significant role to play in the perception towards the security and privacy issues. SNS are very popular among the graduates and post graduates and are more or less used for fun and entertainment, making new relations and social purpose and marketing. Most of the users have been using them for a long time and also spend a significant amount of their time on these sites. Users of SNS are fearful about photos and other articles being downloaded about information displayed being inappropriately used by others about intellectual rights being infringed, copied or abused by others, about identity theft, profiling or phishing and a significant concern that the SNS provider might divulge information to other parties without ones explicit consent. Different demographics have a different impact on the perception towards security and privacy issues. The concern towards who one was talking to when online was less but in the other cases the concern was significantly high.

Management Implications

The study could have serious management implications for the users as well as the providers. The users could be caution about the kind of information they are sharing so that any possibility of their misuse could be avoided. Any kind of controversial photographs could be avoided being posted, any issues relating to security and privacy issues could be avoided, matters involving IPRs need not be shared and the like. SNS are very user friendly and would motivate and motivate the users to share as much as information as possible. But it is for the users to avoid posting information which is controversial or could induce malicious usage. The service providers could also understand the perception of the users of SNS regarding their concern for security and privacy issues and thereby design usages so that they could attract more number of users. The companies could also understand the concern of the users and makes their product accordingly**.**

References

Ai Ho, A. M. (2009). Privacy Protection Issues in Social Networking Sites . *IEEE* , 271-278.

Aimeur, E. G., & Ho, A. (2010). Towards a Privacy-Enhanced Social Networking Site. *Availability, Reliability, and Security* , 172 - 179.

ISSN 2348–0661 Print

Alessandro Acquisti, R. G. (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. *Springer , 4258*, 36-58.

Alyson L. Young, A. Q.-H. (2009). Information revelation and internet privacy concerns on social network sites: a case study of facebook. *fourth international conference on Communities and technologies* , 265-274 .

Amin Tootoonchian, S. S. (2009). Lockr: better privacy for social networks. *5th international conference on Emerging networking experiments and technologies* , 169-180 .

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

Carlos Flavián, M. G. (2006). Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site. *Industrial Management & Data Systems , 106* (5), 601 - 620.

Cutillo, L. R., & Strufe, T. (2009). Safebook: A privacy-preserving online social network leveraging on real-life trust. *Communications Magazine, IEEE , 47* (12), 94 - 101.

Gartrell, M., & Han, R. (2009). Solutions to Security and Privacy Issues in Mobile Social Networking. *Computational Science and Engineering , 4*, 1036 - 1042.

Hasib, A. A. (2008). Threats of Online Social Networks. *Seminar on Internetworking* .

Katherine Strater, H. R. (2008). Strategies and struggles with privacy in an online social networking community. *22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction* , 111-119 .

Kevin Lewis, J. K. (2008). The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network. *Journal of Computer-Mediated Communication , 14* (1), 79–100.

Matthew M. Lucas, N. B. (2008). FlyByNight: mitigating the privacy risks of social networking. *7th ACM workshop on Privacy in the electronic society* , 1-8.

Molva, R., & Strufe, T. (2009). Privacy preserving social networking through decentralization. *Wireless On-Demand Network Systems and Services* , 145 - 152.

Pelgrin, W. F. (2010). Security and Privacy on Social Networking Sites. *Multi-state information sharing and analysis centre , 5* (3).

Ralph Gross, A. A. (2005). Information revelation and privacy in online social networks. *ACM workshop on Privacy in the electronic society* , 71-80.

ISSN 2348–0661 Print

Shin, D.-H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with Computers , 22* (5), 428–438.

Williams, J. (2010). Social networking applications in health care: threats to the privacy and security of health information. *ICSE Workshop on Software Engineering in Health Care* , 39-49.

Xie, Q., & Hengartner, U. (2009). FaceCloak: An Architecture for User Privacy on Social Networking Sites. *Computational Science and Engineering , 3*, 26-33.

ISSN 2348–0661 Print