IBIMA Publishing
Journal of Internet Social Networking & Virtual Communities
http://www.ibimapublishing.com/journals/JISNVC/jisnvc.html
Vol. 2012 (2012), Article ID 281869, 11 pages
DOI: 10.5171/2012.281869

Examining Information Disclosure Behavior on Social Network Sites Using Protection Motivation Theory, Trust and Risk

Norsaremah Salleh[1], Ramlah Hussein[2], Norshidah Mohamed[3], Nor Shahriza Abdul Karim[3], Abdul Rahman Ahlan[1] and Umar Aditiawarman[1]

[1]International Islamic University, Malaysia

[2]Sri Jentayu Sdn Bhd, Malaysia

[3]Universiti Teknologi, Malaysia

Abstract

This paper reports on an empirical study that investigates the information disclosure behavior on Social Network Sites (SNS) focusing on undergraduate University students as our population. Although much have been reported on the issue of information privacy or privacy leakage on SNS, very few have employed the Protection Motivation Theory (PMT) as a framework to understand SNS user's behavior related to information disclosure. In this study, the PMT incorporated with trust and risk factor, has revealed that trust on SNS and perceived benefits influenced information disclosure behaviour. Our findings showed that all PMT constructs are significantly related to privacy concern. However, privacy concern and perceived risk were found not related to information disclosure behaviour. Using self-administered questionnaire, 486 undergraduate students from five different universities in Malaysia were involved in this study.

Keywords: Protection Motivation Theory, privacy concern, perceived risk, trust.

Introduction

The Social Network Sites (SNS) such as Facebook, MySpace, Twitter, Friendster, etc. have become an unprecedented phenomenon which has transformed the way people communicate and interact with others. A growing number of SNS users over time indicate that people have gained the benefit from using SNS services. The Facebook statistics at the end of December 2011 show that there are 845 million monthly active users and more than 50% of monthly active users accessed the site from their mobile phone (www.facebook.com).

In order to use SNS, a person needs to provide his/her personal information to SNS company for a registration purpose. After the new SNS account has been validated through e-mail, the new user should be able to create his/her profile by customizing the personal information they want to reveal and to whom the information is available. With this practice, users can interact and make friends more easily and conveniently.

Apart of the advantages that can be obtained by the SNS users from sharing personal information, SNS may become potentially vulnerable to privacy violation as it does not rule the use of one's information (e.g. picture, name, etc.) by other SNS user without any consent. Although SNS by itself is equipped with systematic safety features, it can not guarantee one's privacy is fully protected. Thus, how much personal information needs to be disclosed should be determined by one's assessment of the benefits and the threats from engaging in risky situation.

The objective of this study is to investigate factors contributing to user's behaviour in disclosing his/her personal information on SNS. The main contribution of this study is to provide a framework that could be used to understand user's protective behaviour pertaining to information disclosure on SNS.

Theoretical Framework

Protection Motivation Theory (PMT)

This study is solely conceptualized on Protection and Motivation Theory (PMT) developed by Rogers (1983). To some extent, the PMT will be incorporated with other factors that can explain user's protective behaviour from engaging in risky activities in SNS. The PMT postulates that one's motivation to protect himself/herself from a risky situation is determined by threat and coping appraisals. The threat appraisals consist of perceived vulnerability and perceived severity, meanwhile coping appraisals consist of self-efficacy and response efficacy. Perceived severity refers to one's perception of the level of damage which may result from engaging in risky situation; meanwhile perceived vulnerability refers to one's perception of experiencing possible negative consequences from performing risky behaviour.

The PMT has been applied widely in the psychology, health-related and environmental research. In the context of Information Systems (IS), the PMT has been used to examine user's protective behaviour in online transaction (LaRose et al., 2006; Youn, 2009), employee's awareness to organizational information security policies (Herath & Rao, 2009; Siponen et al., 2010) and individual use of security software (Johnston & Warkentin, 2010).

However, only few studies found applying the PMT to explain users' protective behaviour associated with information disclosure in SNS. Several studies used PMT constructs and incorporated with other factors associated with information disclosure behaviour such as privacy concern (Young & Haase, 2009; Acquisti & Gross, 2006), locus of control (Lo, 2010), and trust (Dwyer et al., 2007). By using PMT and social influence as a framework, Banks et al. (2010) examine information sharing behaviour in SNS. They investigated how SNS users perform a mental calculation by trading-off the potential vulnerability and severity of the threat with the rewards associated with risky behaviour. The findings uncovered that perceived vulnerability, severity and rewards associated with information sharing contribute to individual's assessment of the threats. It implies that rewards countervail the effect of perceived severity and vulnerability resulting in a lower threat assessment and hence elevate motivation to engage in the behaviour. However, their study only focused on threat appraisals without investigated further the role of coping appraisals in protective behaviour.

Somehow, individual's coping appraisal associated with information disclosure needs to be investigated to understand one's protective behaviour in SNS. Researchers found that self-efficacy, which refers to individual's belief in his/her ability to perform a particular task, plays an important role in explaining protective behaviour (LaRose et al., 2006; Youn, 2009). Self-efficacy of information disclosure refers to one's belief in his/her ability to protect his/her privacy from illegal practice of information collection and sharing activities. This can be associated to one's awareness of using privacy protection features provided in SNS. On the other hands, response efficacy refers to the degree to which an individual believes the response one takes is effective in alleviating the threat (La Rose et al., 2006). Table 1 shows existing literature that have investigated the determinants of information disclosure behavior in SNS.

Table 1. Determinants of Privacy Protection and Information Disclosure Behaviour

Authors	Independent Variable	Dependent Variable	Sample	Method	Findings
Banks et al. (2010)	Realized Threat, Perceived Severity, Perceived Vulnerability, Perceived Rewards, Perceived Threat, Social Influence	Intention to Share Information	Univ. Students (N=197)	Survey Study	All independent variables expalined about 32.1% of the variance in intention to share information on SNS.
Young & Haase (2009)	SNS usage, Personal Network Size, Internet Privacy Concern, Concern about Unwanted Audiences, Privacy Protection Strategies, Profile Visibilities	Information Revelation	Univ. Students (N=77)	Survey Study (questionnaire & Interview)	All independent variables explained about 40.3 % of the variance in informartion revelation on SNS.
Youn (2009)	Gender, Internet Use, Persuasion Knowledge, Privacy Knowledge, Vulnerability to Risks, Information Disclosure Benefits, Privacy Self-efficacy, Online Privacy Concerns	Privacy Protection Behaviour	School Students (N=144)	Survey Study	Perceived vulnerability and information disclosure benefits explain about 24.7% of the variance in privacy concern which is in turn affect privacy protection behaviour.
Lo (2010)	Internet Privacy Concern, Locus of Control, Salience of SNS in daily life, Perceived Risk, Trust in SNS	Information Disclosure	Univ. Community (N=53)	Survey Study	Internet privacy concern, locus of control and salience of SNS explained 44% and 12% of the variance in perceived risk and trust respectively, which is in turn contribute to information disclosure behaviour (R^2=0.240)
Acquisti & Gross (2006)	Privacy Attitudes, Privacy Concerns, SNS Usage, Trust in SNS	Information revelation	University Community (N=294)	Survey Study	Privacy concern is not related to information revelation
Dwyer et al. (2007)	Internet Privacy Concern, Trust in SNS, Trust in other members of SNS	Development of new Relationships, Information Sharing	College Students (N=117)	Survey Study	Partial relationship found between independent and dependent variables
Rifon et al. (2005)	Seal Presence, Privacy Self-efficacy, Site Involvement	Seal Assurance, Trust of the Site, Information Disclosure	University Community (N=210)	Survey Study	Partial relationship found between independent and dependent variables moderated by seal presence

According to Westin (1967), privacy is defined as the desire of people to have the freedom of choice under whatever circumstances and to whatever extent they expose their attitude and behaviour to others. Where the Internet is concerned, privacy concern refers to the user's perception of the likelihood that the internet vendor will try to protect user's confidential information collected during electronic transactions from unauthorized use or disclosure (Kim et al., 2008).

Therefore, for many internet users, privacy loss is the main concern and the need for protection of information transaction is crucial. Privacy violations on the internet include spamming, usage tracking and data collection, and the sharing of information to third parties. When users perceive that their information privacy is being violated, they will be less likely to disclose their personal information to the internet (Dinev & Hart, 2004). In other words, higher privacy concern may be determined by higher perceived vulnerability associated with information disclosure. In line with these reasoning, we propose the following hypotheses:

H1 Perceived vulnerability is positively related to privacy concern of information disclosure.

H2 Perceived severity is positively related to privacy concern of information disclosure.

H3 Privacy self-efficacy is positively related to privacy concern of information disclosure.

H4 Response self-efficacy is positively related to privacy concern of information disclosure.

H5 Perceived benefit is positively related to information disclosure in SNS.

Trust and Perceived Risk

It cannot be denied that trust become pivotal in all daily interactions, communications, and transactions, especially in the virtual environment such as the internet. Mayer et al. (1995) defined trust as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform particular action important to the trustor, irrespective of the ability to monitor or control that other party". Trust is essentially needed only in uncertain situations since trust effectively means to assume risks and become vulnerable to trusted parties Hosmer (1995).

According to Pavlou (2003), trust is found to be a significant antecedent of perceived risk. If there was no risk and actions could be taken with complete certainty no trust would be required. It was found that perceived risk decreases when trust occurs. However, since risk itself is difficult to measure objectively, established research has predominately defined perceived risk as "an individual's subjective expectation of suffering a loss in pursuit of a desired outcome" (Warkentin et al., 2002).

Trust and perceived risk are critical to any online transactions such as e-commerce Pavlou (2003), e-government (Belanger & Carter, 2008), and internet banking (Casalo et al., 2007). In the context of SNS, researchers have investigated the role of trust on information disclosure behaviour. Studies by (Acquisti & Gross, 2006) and (Fogel & Nehmad, 2009) found that majority students in college or university tend to trust Facebook (FB) and its members compared to other SNS (MySpace, Friendster). However, these findings are merely based on descriptive analysis. They did not perform further analysis to explain a causal relationship of trust factor or even the role of trust on information disclosure.

Dwyer et al. (2007) investigate the impact of trust on information disclosure between FB and MySpace users. In their study, trust is divided into two dimensions; trust of the SNS system and trust of the SNS members. Despite the findings revealed the correlation between trust of SNS and information sharing, the trust factors do not represent the overall picture of trust in SNS. As reported, both of trust constructs found to be less reliable and seemed not adaptable for future study. Recent study by Lo (2010) revealed significant relationship between trust and willingness to provide information on SNS. The findings imply that trust is driven by SNS system capability in protecting and managing the personal information. As a result, it elevates the level of confidence to disclose the personal information and in turn lowers the risk level. With above reasoning, we hypothesized:

H6 Perceived vulnerability is positively related to perceived risk of information disclosure.

H7 Perceived severity is positively related to perceived risk of information disclosure.

H8 Privacy self-efficacy is positively related to perceived risk of information disclosure.

H9 Response self-efficacy is positively related to perceived risk of information disclosure.

With regard to privacy concern of information disclosure, trust is believed to have an impact on information disclosure behaviour. If the users perceive that the SNS care about information privacy, honest and competence in protecting personal information, the level of concern over privacy is likely lower Xu (2009). Thus, we hypothesized:

H10 Privacy concern is negatively related to information disclosure.

H11 Perceived risk is negatively related to information disclosure.

H12 Trust in SNS is positively related to information disclosure.

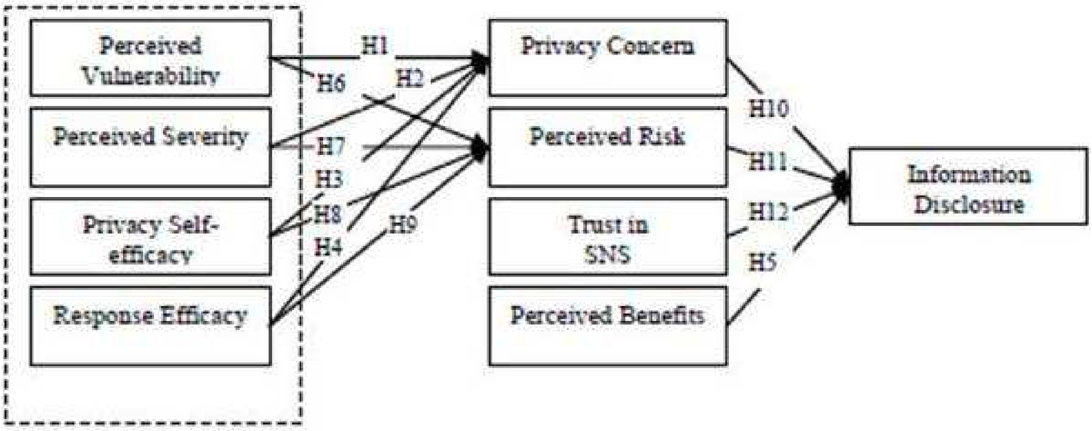

Fig1. Research Model

Research Methodology

This study employs a survey method to gather the information from the respondents. Self-administered questionnaire was performed targeting university's students as sample. A total of 500 questionnaires were distributed to students from both public and private universities in Malaysia. A random sampling technique is adopted for questionnaire distribution. Prior to actual data collection, a pilot study is conducted to reduce biases in format and content of the instruments.

Based on the proposed model, there are eight main constructs deployed in this study. The questions are adopted and adapted from previous studies that have empirically validated the instruments. A six point-likert scale is applied for each item of the questionnaire except items in demographic section. The likert-scale is ranging from 1=strongly disagree to 6=strongly agree. To measure "Perceived Vulnerability", "Privacy Self-efficacy" and "Response Efficacy", this study adapts the instruments from (Youn, 2009; Dinev & Hart, 2004; Rogers, 1997). The construct of "Perceived Severity" and "Perceived Benefits" are derived from (Banks et al., 2010). The "Perceived Risk" and "Trust on SNS" construct are adapted from the study by (Pavlou, 2003; Lo, 2010). "Privacy Concern" associated with information disclosure is examined with seven items. The study adapts the construct from Fogel & Nehmad (2009) and Xu (2008). Lastly, to examine "Information Disclosure" behavior, this study adapts the instruments from Lo (2010).

Pilot Study

Pilot study was conducted to ensure the quality of the instruments before deploying the questionnaire to actual respondents. Sixteen participants comprised undergraduate students were voluntarily participated and selected randomly in the pilot study. The reliability test was performed using SPSS (release 19) for Windows to evaluate the measurements.

A Cronbach alpha technique is used. According to Hair et al. (1998), if the factor scores above 0.7 of the Cronbach alpha values is considered as reliable. Most of the constructs employed in the study are reliable (α>0.7), except for Privacy Self-efficacy (α=0.341). This is due to number of items being used only two. Researchers agreed to examine further this construct before conducting the actual survey.

Survey

Total of 492 participants returned the questionnaire. Due to providing typical answer on every field and unanswered questions, only 486 questionnaires will be used for further analysis representing of 97% of target sample. The demographic profile of the respondents is shown in Table 2. As can be seen, most of the respondents have been using the SNS for three years and above. From the preliminary question, majority of students are aware of their information privacy on SNS (88.3%). This is shown also by how they use the privacy settings provided by the SNS. According to our survey, most of the students have multiple SNS accounts. About 472 of our respondents have Facebook account followed by Twitter (N=162) and MySpace (N=139). Students will spend about 1 to 3 hours a day accessing the SNS through their own laptop or smart phones.

Table 2. Demographics of the Respondents

Item		**Frequency**	**%**
Gender	Male	199	40.9
	Female	287	59.1
Age	<20	159	32.7
	20-24	295	60.7
	25-30	15	3.2
	>30	2	0.4
Race	Malay	434	89.3
	Chinese	18	3.7
	Indian	21	4.3
SNS usage (years)	<1	13	2.7
	1-3	262	53.9
	4-6	141	29.0
	>6	44	9.1
Privacy awareness in SNS	Yes	429	88.3
	No	51	10.5
Privacy features use	Yes	412	84.8
	No	63	13.0

Data Analysis

The first step of the analysis is to test the validity of the measurements employed in the study. The main purpose of this analysis is to validate whether a measure of a concept really measure the concept being studied. Construct validity analysis is performed to examine the degree whether a measure relates to other factors as expected within a system of theoretical relationships. A principal component method analysis is used with varimax rotation to test the correlation among the factors. The appropriate cut-off significant loading based on the sample size of this study is 0.4 [Hair et al., 1998). Table 3 summarizes the results of factor analysis suggesting that the measurement exhibited somewhat suitable for the context of this study.

As can be seen all the items loaded according to its respective factors except items fall under “Perceived Severity” and “Perceived Vulnerability”. Perceived vulnerability on SNS refers to one’s perception of experiencing possible negative consequences from disclosing personal information, while perceived severity refers to the level of damage caused by disclosing personal information.

Table 3. Factor Loadings

	Factor							
	1	2	3	4	5	6	7	8
PC4	.797							
PC5	.790							
PC3	.784							
PC2	.775							
PC8	.774							
PC6	.697							
TRS6		.808						
TRS5		.805						
TRS2		.757						
TRS3		.756						
TRS4		.751						
TRS7		.749						
TRS1		.695						
PSEV1			.749					
PSEV3			.734					
PSEV2			.711					
PV2			.528					
PV1			.527					
PSE2				.754				
PSE3				.730				
PSE5				.710				
PSE1				.667				
PSE6				.647				
PSE4				.535				
ID2					.827			
ID4					.807			
ID3					.788			
ID5					.741			
ID1					.689			
ID6					.576			
RSK1						.813		
RSK2						.798		
RSK3						.774		
RSK4						701		
PB2							.844	
PB3							.813	
PB1							.726	
PB4							.704	
RE2								.727
RE1								.713
RE4								.700
RE3								.693

(PC) Privacy Concern (TRS) Trust (PSEV) Perceived severity
(PV) Perceived Vulnerability (PSE) Perceived Self-Efficacy
(ID) Information Disclosure (RSK) Perceived Risk
(PB) Perceived Benefits (RE) Perceived Response-Efficacy

In this study, respondents perceived both measures are explaining the same factor where the potential negative consequences is highly associated with level of damage if one’s perform a risky behaviour such as providing a real name, photograph, email address, etc. at profile section. As the items merged in one factor, we will call this factor as Perceived Severity and Vulnerability (PSV) from herein. Next, Cronbach Alpha was used to assess the reliability of the construct. Each item was assessed by examining the loadings of the items on their respective constructs. As depicted in Table 4, all the factors scored relatively high (α>0.7) ranging between 0.839 and 0.905. The reliability test indicates that all the constructs are reliable and suitable to measure the concepts employed in the study.

Table 4. Reliability Analysis

Measurements	***No. items***	***Cronbach Alpha***
Privacy Concern (PC)	6	0.901
Trust (TRS)	7	0.905
Risk (RSK)	4	0.905
Self-efficacy (PSE)	6	0.847
Perceived Severity & Vulnerability (PSV)	5	0.854
Response Efficacy (RE)	4	0.905
Perceived Benefits(PB)	4	0.875
Information Disclosure (ID)	6	0.839

To test the hypotheses underlying the proposed model, correlation analysis was conducted. Correlation analysis was used to determine the association among all the factors investigated under this study. Four factors: "Perceived Risk", "Privacy Concern", " Trust on SNS", and "Perceived benefits" have been identified as independent variables which expected to influence "Information Disclosure Behaviour", as dependent variable. This study also interested in explaining the role of individual's protection motivation pertaining to the information disclosure on SNS.

The result exhibits that perceived benefits (r=0.210) and trust on SNS (r=0.183) are moderately related to information disclosure behavior (see Table 5). This indicates that by providing personal information such as real name, photograph, affiliation, email, etc., he/she will be acknowledged as genuine person and will be easier to find old/new friends on SNS. Another benefit perceived by respondents from sharing personal information is to get an acquaintance in a group or community created in SNS. The result also discovers that SNS are trustworthy in handling personal information and considered as a safe environment to interact among SNS users. The SNS companies have assured its members that legal and technological structure to protect personal information is preserved by providing privacy settings which tied up with the current practice of online privacy policy. Thus, hypotheses H5 and H12 are supported in the study.

Surprisingly, perceived risk (r=-0.053) and privacy concern (r=0.028) are not related to information disclosure 8behavior. This result somehow contradicts with several previous studies on SNS (Fogel & Nehmad, 2009; Lo, 2010). Lo (2010) demonstrated that privacy concern is positively related to risk and negatively correlated with trust which in turn influences individual willingness to provide personal information. Another study by Fogel & Nehmad (2009) found the difference between men and women in protecting their online privacy. Even women are reassured about privacy protection on SNS, they are unlikely to disclose real information compared to men. However, Acquisti & Gross [19] argued that generally SNS members unaware of the stated privacy policy and most of them believed that SNS do not share personal information to third parties. They also believed on their ability to control personal information through SNS privacy setting which eventually will alleviate their concern on information privacy. Thus, based on our data, H10 and H11 are not supported under this study.

It was admitted in the past the development of SNS structure merely focus on facilitating people to get to know each other or just to find old/new friends without discerning the online privacy. As a number of SNS memberships growing rapidly, information privacy become important element that needs to be protected by SNS companies. With regard to the role of PMT as antecedent of privacy concern, the result demonstrates that all PMT constructs are significantly related to privacy concern. In other words, respondents have considered threat and coping appraisals prior to engage in SNS environment. It implies that possible negative consequences and the level of damage caused by providing real personal information on SNS have been realized at the first stage. To countervail such threat in SNS, respondents believe at their ability to protect their personal information by enabling the privacy protection measures provided in SNS.

PMT constructs are also believed influencing perceived risk of information disclosure. The result demonstrates that perceived severity and vulnerability is positively related to perceived risk. It implies that respondents concede by engaging in risky behavior such as revealing personal information can be resulted in serious consequences (e.g. identity theft, virus, hacking, etc.).

Table 5. Correlation Analysis

	PC	TRS	RSK	PSE	RE	PB	PSV	ID
PC	1							
TRS	.124**	1						
RSK	.533**	.164**	1					
PSE	.273**	.560**	.332**	1				
RE	.424**	.434**	.482**	.550**	1			
PB	.343**	.354**	.321**	.380**	.540**	1		
PSV	.588**	.228**	.601**	.404**	.583**	.467**	1	
ID	.028	.183**	.053	.140**	.083	.210**	.045	1

(PC) Privacy Concern (TRS) Trust (RSK) Perceived Risk
(PSE) Perceived Self-Efficacy (RE) Perceived Response-Efficacy
(PB) Perceived Benefits (PSV) Perceived Severity & Vulnerability
(ID) Information Disclosure

Conclusion

The objective of this study is to investigate the role of individual's protection motivation, privacy concern, trust and perceived risk on information disclosure behaviour in SNS. The findings show that trust on SNS and perceived benefits determine one's behaviour to reveal or share the real personal information in SNS, while perceived risk and privacy concern do not influence information disclosure behaviour. The findings have also validated the relationship between PMT constructs and perceived risk and privacy concern. It is suggested that protection motivation behaviour play an important role on privacy concern especially when dealing with risky behaviour. However, our study reveal that sharing information on SNS is not considered as risky behaviour, thus privacy is likely not the main concern.

This study was conducted in Malaysia targeting youngster as sample of the study. Although SNS are quite popular among the youngster, comparing this findings with elder people who used SNS may give a new insight. We suggested future study to look into other factors that are believed influencing information disclosure behaviour in SNS such as the use of SNS privacy and security features, user locus of control, social influence.

In conclusion, this study has provided another insight in SNS research area. Through empirical data analysis, this study has supported several studies on SNS information disclosure as well as refuted other indications found in the past research. A non-standard policies and privacy protection measures provided by SNS may baffle the perception about all factors presented in this study. We hope further study will be focusing on specific SNS and other features of SNS involving privacy.

Acknowledgment

This research is funded by the Fundamental Research Grant Scheme (FRGS11-010-0158) of the Ministry of Higher Education Malaysia.

References

Acquisti, A. & Gross, R. (2006). "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," *Privacy Enhancing Technologies*, pp. 1-22.

Banks, M. S., Onita, C. G. & Meservy, T. O. (2010). "Risky Behaviour in Online Social Media: Protection Motivation and Social Influence," *AMCIS 2010 Proceedings*.

Belanger, F. & Carter, L. (2008). "Trust and Risk in e-Government Adoption," *Journal of Strategic Information Systems*. 17(2), 1-15.

Casalo, L. V., Flavian, C. & Guinaliu, M. (2007). "The Role of Security, Privacy, Usability and Reputation in the Development of Online Banking," *Online Information Review, 31(5), 583-603*.

Dinev, T. & Hart, P. (2004). "Internet Privacy Concerns and Their Antecedents Measurements Validity and Regression Model," *Behaviour & Information Technology, vol. 23, no. 5, pp. 413-422*.

Dwyer, C., Hiltz, S. & Passerini, K. (2007). "Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace," *AMCIS 2007 Proceedings*.

Fogel, J. & Nehmad, E. (2009). "Internet Social Network Communities: Risk Taking, Trust, and Privacy Concerns," *Computer in Human Behaviour, vol. 25, pp. 152-160*.

Hair, J. F., Anderson, R. E., Tatham, R. L. & Black, W. C. (1998). Multivariate Data Analysis, New Jersey: *Prentice Hall*.

Herath, T. & Rao, H. R. (2009). "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems*, 18(2), 106-125.

Hosmer, L. T. (1995). 'The Connection Link between Organizational Theory and Philosophical Ethics,' *Academy of Management Review*. 20(3). 213-237.

Johnston, A. & Warkentin, M. (2010). 'Fear Appeals and Information Security Behaviours: An Empirical Study,' *MIS Quarterly*, 34(1).

Kim, D. J., Ferrin, D. L. & Rao, H. R. (2008). "A Trust-Based Consumer Decision-Making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents," *Decision Support Systems*, 44, 544-564.

LaRose, R., Rifon, N. J. & Enbody, R. . (2008). "Promoting Personal Responsibility for Internet Safety," *Communication of the ACM, vol. 51, no. 3, pp. 71-76*.

Lo, J. (2010). "Privacy Concern, Locus of Control, and Salience in a Trust-Risk Model of Information Disclosure on Social Networking Sites," *AMCIS 2010 Proceedings*.

Mayer, R. C., Davis, J. H. & Schoorman, F. D. (1995). "An Integrative Model of Organizational Trust," *Academy of Management Review*, 20(3), 709-734.

Pavlou, P. A. (2003). "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model," *International Journal of Electronic Commerce*. 7(3). 101-134.

Rifon, N. J., LaRose, R. & Choi, S. M. (2005). "Your Privacy is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures," *The Journal of Consumer Affairs*, 39(2), 339-362.

Rogers, R. W. (1983). 'Cognitive and Physiological Processes in Fear Appeals And Attitude Change: A Revised Theory of Protection Motivation,' *Social Psychophysiology*, pp. 153-176.

Rogers, R. W. & Prentice-Dunn, S. (1997). “Protection Motivation Theory,” *Handbook of Health Behaviour Research*, 1, 113-132.

Siponen, M., Pahnila, S. & Mahmood, M. A. (2010). “Compliance with Information Security Policies: An Empirical Investigation,” *Computer*, pp. 64-71.

Stutzman, F. (2005). 'An Evaluation of Identity-Sharing Behavior in Social Network Communities,' Ibiblio.org. Retrieved October 2, 2006 .

Warkentin, M. Gefen, D., Pavlou, P. A. & Rose, G. M. (2002). ”Encouraging Citizen Adoption of e-Government by Building Trust,” *Electronic Markets*. 12(2). 157-162.

Westin, A. F. (1967). “Privacy and Freedom,” *New York: Atheneum*.

Wirth, C. B., Rifon, N. J., LaRose, R. & Lewis, M. L. (2007) “Promoting Teenage Online Safety with an i-Safety Intervention Enhancing Self-efficacy and Protective Behaviour,” available at: https://www.msu.edu/~wirthch1/childsafety07.pdf (accessed March 17, 2011).

Xu, H. (2009). “Consumer Responses to the Introduction of Privacy Protection Measures: An Exploratory Research Framework,” *International Journal of E-Business Research*, 5(2), 21-47.

Xu, H., Dinev, T. , Smith, H. J. & Hart, P. (2008). “Examining the Formation of Individual’s Privacy Concerns: Toward an Integrative View,” *ICIS Proceedings*.

Young A. L. & Quan-Haase, A. (2009). “Information revelation and internet privacy concerns on social Network Sites: A Case Study Of Facebook,” Proceedings of the fourth international conference on Communities and technologies, pp 265-274.

Youn, S. (2009). “Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviour among Young Adolescents,” *The Journal of Consumer Affairs, vol. 43, no. 3, pp. 389-418*.