Information Disclosure Behaviour in Social Media among Malaysian Youth: The impact of Privacy Concern, Risk and Trust

Norsaremah Salleh
Department of Computer Science
International Islamic University Malaysia
norsaremah@iium.edu.my

Umar Aditiawarman
Department of Information Systems
International Islamic University Malaysia
oemar99@gmail.com

Ramlah Hussein
School of Computer Technology
Sunway University
Petaling Jaya, Malaysia
ramlahh@sunway.edu.my

***Abstract*— People have been using Social Network Sites (SNS) to communicate and make friends through online. Although SNS has been benefited its users in many ways, information privacy seemed to be overlooked. This study proposes a framework to examine users' protective behaviour associated with information disclosure in SNS. The proposed framework was derived based on the Protection Motivation Theory and Privacy Concern.**

Keywords-component: Privacy concern, perceived risk, trust, privacy self-efficacy, perceived vulnerability

I. INTRODUCTION

Social Network Sites (SNS) such as Facebook, MySpace, Twitter, Friendster, etc. have become an unprecedented phenomenon that transform the way people communicate and interact with others. A growing number of Facebook users over time indicate that people have gained the benefit from its services. The Facebook claimed per March 2011 that it has more than 640 millions users whom 50% active users and 10% accessed from mobile phone (www.facebook.com).

In order to use SNS, potential users need to provide their personal information to SNS for a registration purpose. After the new account is confirmed through e-mail, users can edit their personal details by customizing the 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.

The objectives of this study are to investigate how far the users aware of information privacy and disclosure on SNS. The main contribution of this study is to provide a framework that could be used to understand users' protective behaviour in relation to information disclosure on SNS.

II. THEORETICAL FRAMEWORK

A. Protection Motivation Theory (PMT) and Privacy Concern

This study is solely conceptualized by Protection and Motivation Theory (PMT) developed by Rogers [25]. To some extent, the PMT will be incorporated with other supporting factors that are believed can explain users' perception of privacy and security awareness 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 include self-efficacy and response efficacy. Perceived severity is 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 areas. In the context of Information Systems (IS), the PMT has been used to examine user's protective behaviour in online transaction (e.g. [2], [3], [4]), employee's awareness to organizational information security policies (e.g. [5], [6]) and individual use of security software [7].

However, only few studies found applying the PMT to explain users' protective behavior associated with information disclosure in SNS. Banks et al. [8] study focused on information sharing behaviour in SNS by using PMT and social influence as a framework. 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.

Somehow, individual's coping appraisal associated with information disclosure needs also be investigated to understand one's protective behaviour in SNS. Researchers found that self-efficacy, which refers to individual's belief in their capability to perform a particular task, play an important role in explaining protective behaviour [3], [4], [9]. Self-efficacy of information disclosure refers to one's confidence in their abilities to protect their privacy from illegal practice of information collection and sharing activities.

According to Westin [10], 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 [11]. Therefore, for many internet users, privacy loss is a main concern and the need for protection of information transaction is crucial. Privacy issues on the internet include spam, usage tracking and data collection, and the sharing of information to third parties. When users perceive that their information privacy is misused by third party, they will be less likely disclose their personal information to the internet [12]. In other words, higher privacy concern may be determined by higher perceived vulnerability associated with information disclosure. Consequently, users tend to avoid exploiting their confidential information and share to public. In line with these reasoning, we propose the following hypotheses:

H1: Perceived vulnerability is positively related to privacy concern of information disclosure.
H2: Privacy self-efficacy is positively related to privacy concern of information disclosure.
H3a: Perceived benefit is negatively related to privacy concern of information disclosure.
H3b: Perceived benefit is positively related to information disclosure.
H4: Privacy concern is negatively related to information disclosure.

B. Trust and Perceived Risk

The dimensions of trust and perceived risk are believed contributing to user's disclosure of personal information on SNS. It cannot be denied that trust become a central issue in all daily interactions, communications, transactions and practices, especially in the remote condition such as the internet. Mayer et al. [13] 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 [14]. According to Pavlou [15], 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" [16].

Trust and perceived risk were found as pivotal factors in any online transactions such as e-commerce [15], e-government [17], and internet banking [18]. In the context of SNS, researchers have investigated the role of trust on information disclosure behaviour. Trust and perceived risk associated with information disclosure in SNS need to be examined to explain. Studies of SNS by [19] and [20] found that majority students in college or university tend to trust Facebook (FB) and its members compared to other SNS (e.g. MySpace, Friendster).

However, the 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. In response to their study, [21] investigate the impact of trust on information sharing or 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 an overall picture of SNS trusting believe. As reported, both of trust constructs found to be less reliable and seemed not adaptable for future study. Recent study by [22] 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.

In relation to privacy concern of information disclosure, trust is believed to have an impact on users' 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 [23]. Figure 1 shows the proposed research model of our study. The relationships among constructs used in our study are to be tested using the following hypotheses:

H5a: Trust is negatively related to perceived risk.
H5b: Trust is positively related to information disclosure.
H5c: Trust is negatively related to privacy concern of information disclosure.
H6: Perceived Risk is negatively related to information disclosure.

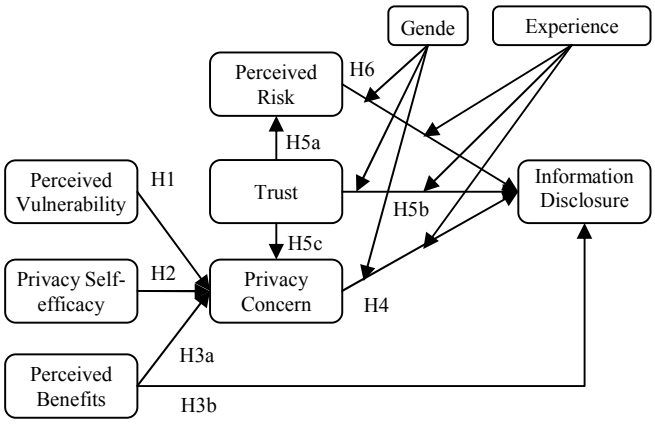

Figure 1. Proposed Research Model

III. RESEARCH DESIGN

This study will employ a survey method to gather the information from the participants. Self-administered questionnaire will be performed targeting university's students as sample. A total of 500 questionnaires will be distributed to students from both the public and private universities. A random sampling technique is adopted for questionnaire distribution. Prior to actual data collection, a pilot study need to be conducted to test the reliability of the instruments. For this purpose, a Cronbach alpha technique is used. According to Hair et al. [24], if the factor scores above 0.7 of the Cronbach alpha values, then it is considered as reliable.

Based on the proposed model, there are seven main constructs involved in the study. The questions are adopted and adapted from previous studies that have empirically validated the instruments. To measure "Perceived Vulnerability" and "Privacy Self-efficacy", this study adapts the instruments from [12] and [4]. The "Information Control" construct is adapted from studies by [12] and [26]. The "Perceived Risk" construct consists of two items derived from the study by [15]. "Privacy Concern" associated with information disclosure is examined with seven items. The study adapts the construct from [26] and [20]. Lastly, to examine "Information Disclosure" behavior, this study adapts the instruments from [22].

ACKNOWLEDGEMENT

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

REFERENCES

[1] R.W. Rogers, "Cognitive and Physiological processes in fear appeals and attitude change: A revised theory of Protection Motivation", *Social Psychophysiology,* pp. 153-176, 1983.
[2] C.B. Wirth, N.J. Rifon, R. LaRose, M.L. Lewis, "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).
[3] R. LaRose, N.J. Rifon, R. Enbody, "Promoting Personal Responsibility for Internet Safety", *Communication of the ACM,* vol. 51, no. 3, pp. 71-76, 2006.
[4] S. Youn, "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, 2009.
[5] M. Siponen, S. Pahnila, M.A. Mahmood, "Compliance with Information Security Policies: An Empirical Investigation", *Computer,* pp. 64-71. 2010.
[6] T. Herath, H.R. Rao, "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations" *European Journal of Information Systems,* 18(2), 106-125, 2009.
[7] A. Johnston, M. Warkentin, "Fear Appeals and Information Security Behaviours: An Empirical Study", *MIS Quarterly,* 34(1), 2010.
[8] M.S. Banks, C.G. Onita, T.O. Meservy, "Risky Behaviour in Online Social Media: Protection Motivation and Social Influence", *AMCIS 2010 Proceedings,* 2010.
[9] N.J. Rifon, , R. LaRose, M.L. Lewis, "Resolving the Privacy Paradox: Toward a Social-Cognitive Theory of Consumer Privacy Protection". available at: https:// www.msu.edu/~wirthch1/privacyparadox07.pdf (accessed March 17, 2011)
[10] A. Westin, "Privacy and Freedom", New York: Atheneum, 1967.
[11] D.J. Kim, D.L. Ferrin, H.R. Rao, "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, 2008.
[12] T. Dinev, P. Hart, "Internet privacy concerns and their antecedents measurements validity and regression model", Behaviour & Information Technology, vol. 23, no. 5, pp. 413-422, 2004.

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

[14] L.T. Hosmer, "The Connection Link between Organizational Theory and Philosophical Ethics", *Academy of Management Review.* 20(3). 213-237, 1995.

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

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

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

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

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

[20] J. Fogel, E. Nehmad, "Internet Social Network Communities: Risk taking, Trust, and Privacy Concerns", *Computer in Human Behaviour*, vol. 25, pp. 152-160, 2009.

[21] C. Dwyer, S. Hiltz, K. Passerini, "Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and Myspace", *AMCIS 2007 Proceedings,* 2007.

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

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

[24] J. Hair, R. Anderson, R. Tatham, W. Black, "Multivariate Data Analysis", *New Jersey: Prentice Hall,* 1998.

[25] R.W. Rogers, S. Prentice-Dunn, "Protection Motivation Theory", *Handbook of Health Behaviour Research,* 1, 113-132, 1997.

[26] H. Xu, T. Dinev, H.J. Smith, P. Hart, "Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View", *ICIS Proceedings*, 2008.