Motivational Factors in Privacy Protection Behaviour Model for Social Networking

Muliati Sedek[1,*], *Rabiah* Ahmad[2], and *Nur Fadzilah* Othman[2]

[1]Center for Teaching and Learning, Universiti Teknikal Melaka, Universiti Teknikal Melaka, 76100 Durian Tunggal, Melaka
[2]Information Security and Networking Research Group (InForSnet), Center for Advanced Computing Technology, Faculty of Information Technology and Communication, Universiti Teknikal Melaka, 76100 Durian Tunggal, Melaka

Abstract. This study aims to investigate the determinants of the privacy protection behaviour strategies that been employed by users while utilising SNSs. By understanding the determinants of privacy protection will be able to generate awareness that can protect users and allow them to confidently impose their self-control through the execution of privacy protection behaviour strategies. The finding has shown that there was a significant relationship of perceived severity, perceived vulnerability, response efficacy and self-efficacy towards information privacy concern as well as a significant relationship of information privacy concern and privacy protection behaviour strategies. This research is crucial as it serves as a guide that provides instructions and guidelines that help users of SNSs to keep their privacy intact.

1 Introduction

Social Networking Sites (SNSs) have become a phenomenon amongst Malaysians. Statistics from the Malaysian Communication and Multimedia Commission (MCMC) has reported that 45.5% of the population or 13.3 million users are registered Facebook users (MCMC, 2014). SNSs such as Facebook and Instagram allow individuals to stay in touch with their friends, reconnect with old friends and create new relationships with other people through the plethora of activities provided, such as sharing photos and videos, archiving events, updating others on activities, sending messages privately and posting public testimonials (Boyd, 2008; Vithessonthi, 2010). Therefore, the nature of SNSs that offer an attractive way of online interaction and communications encourage users to use it to its zenith. Unfortunately, the excessive information sharing and activities performed while accessing SNSs in an uncontrolled manner, can lead to a privacy breach on the user's behalf.

Recently, privacy issues related to personal information has been widely discussed and deliberated by various researchers (Nemec Zlatolas, Welzer, Heričko, & Hölbl, 2015). Due to the rapid development and utilisation of communication technology, privacy has become a serious concern. Users are willingly to share their private information subconsciously without a clear idea of who is allowed to access to their personal information and what portion of it is really accessed. Even though SNSs themselves have been equipped with systematic safety features, there is no guarantee that one's privacy is fully protected (Salleh et al., 2012). Hence, there is an urgent need for an assessment mechanism that can detect threats from engaging in risky situations so that users can determine how much and what type of personal information should be shared and disclosed.

Therefore, this study aims to investigate the determinants of the privacy protection behaviour strategies that been employed by users while utilising SNSs. By understanding the determinants of privacy protection will be able to generate awareness that can protect users and allow them to confidently impose their self-control through the execution of privacy protection behaviour strategies.

2 Privacy Protection Behaviour Strategies

Literature has given various definitions of privacy. The concept of privacy ranges from a "right to be alone" as from the perspective of law (Warren & Brandeis, 1890), "state of limited access" in the aspect of philosophy (Schoeman, 1984), and to the "control over information about one's self" as given from the views of social science (Kokolakis, 2017).

Privacy protection behaviour can be defined as specific computer-based actions that individuals take to keep their information safe. Rogers (1983) has discussed that individuals are motivated to rely on protection behaviour in order to cope and adopt behaviour to control risk, threat and danger. Coping strategies can be divided into two dimensions, which are approach and avoidance (Chen, Beaudoin & Hong, 2017). Approach strategies include fabricating personal information and seeking

* Corresponding author: muliati@utem.edu.my

social support whereas avoidance strategies include withholding personal information. In the context of SNS, fabricating information as based on approach strategies refers to a user covering up or disguising their identity by using fake or false information in SNSs. Seeking social support means that users ask for advice and read privacy statements from SNS providers in order to gain knowledge that would help them adopt privacy protection behaviour strategies alongside increasing their privacy. As for avoidance strategies, refraining information means that users will refuse to provide their personal information to SNSs and instead even begin to patronize them over it.

Information privacy concern is the "extent to which an individual is concerned about organizational practices related to the collection and use of his or her personal information (Martin, Borah & Palmatier, 2017). Previous research has shown that information privacy concern has an impact on privacy protection behaviour strategies (Adhikari & Panda, 2017). Within the protection motivation theory, information privacy concern is considered to be a mediating variable that explains the relationship between the factors involved and privacy protecting behaviour strategies.

3 Theoretical Framework and Hypotheses

3.1. Protection Motivation Theory

Protection Motivation Theory (PMT) as introduced by Rogers (1975) postulates that an individual's motivation to protect from risk and threat, which comes from (1) perceived severity, (2) perceived vulnerability and (3) response efficacy. The PMT model was modified to explain failures concerned in protection behaviour by including (4) self-efficacy, (5) response cost and (6) rewards associated with risky behaviour (Rogers, 1983; Rogers, 1975). PMT has been principally used in the health industry (Grindley, Zizzi & Nasypany, 2008) this theory has also been used in more than 20 different health- related areas in order to study about intentions and behaviours. In the field of Information System (IS), PMT has also been widely used to examine protection behaviour in online transactions, awareness of employees in organizational information security policies and individual use of security software (Johnston & Warkentin, 2010).

3.1.1 Perceived Severity

Perceived severity refers to an individual's belief that the judgement of severity significance results from a threatening event (Palladino, BMenesini et al., 2017). Perceived severity evaluated how severe an individual believes that threat will interrupt their life. Individuals will adopt recommended action when they seriously perceive the negative consequence. Moreover, Adhikari and Panda (2017) found that an individual's motivation for engaging in risk-reducing behaviour is increased by perceived severity. For the purpose of this study, users will develop a perceived severity after losing information privacy to SNSs. They will significantly associate this loss with information privacy concern and in this form, indirectly motivate them to adopt privacy protection strategies in SNSs.

3.1.2 Perceived Vulnerability

Perceived vulnerability explains an individual's perception in experiencing possible negative effects that stem from performing risky behaviour (Kim & Kim, 2016). Based on the findings, it can be argued that perceived severity is found to have increased students' intention to perform malware avoidance behaviour. Subsequently, Schoeman (1984) agreed that one of the factors that contribute to users increasing information privacy concerns is perceived vulnerability. Conversely, perceived vulnerability has an insignificant impact on employees' intention to comply with IS security policies (Kokolakis, 2017). Thus, for this study, it is suggested that individuals who perceive the risk and threats of losing information privacy through SNSs will increase their information privacy concerns which will later motivate them to use privacy protection behaviour strategies.

3.1.3 Self-efficacy

Self-efficacy is defined as an individual's belief and capability to implement protective behavior while using SNSs (Compeau, Higgins, & Huff, 1999). Several studies provide evidence that self-efficacy plays an important role in a user's choice to perform risky online behaviour. While Lee et al. (2008), proves that self-efficacy should be the influential factors that stimulates protection behaviour. Hence, this study suggests that individuals who are self-efficacious in using SNSs are more likely concerned with their information privacy and are totally motivated to use privacy protection behaviour strategies.

3.1.4 Response efficacy

Response efficacy is the belief in coping with responses in avoiding a threat (Grindley et al., 2008). Research identifies that response efficacy is a significant predictor behaviour that determines the decision whether or not to implement security features on their networks, increase intentions to use anti-spyware software as protective technology, predicts backing up data on personal computers and use of malware devices (Martin et al., 2017). Therefore, the study posits that by having a good response efficacy could help users in decreasing the loss of data.

3.1.5 Rewards

Reward refers to an individual's expectation in getting benefits when keeping with selective behaviour (Lee et al., 2008). Previous study has shown that individuals who find great enjoyment and satisfaction from sharing personal information are less inclined to make adaptive change for protection (Marett, Harris, & Mcnab, 2011). Additionally, individuals believe that when they are willing to disclose their information, they may experience a sense of being close to their friends and family and at the same time get satisfaction from the feeling of togetherness.

3.2 Information Privacy Concern

Information privacy concern is the "extent to which an individual is concerned about organizational practices related to the collection and use of his or her personal information. Previous research has shown that information privacy concern had an impact on privacy protection behaviour strategies. Within the protection motivation theory, information privacy concern is considered to be a mediating variable that explains the relationship between the factors involved and privacy protecting behaviour strategies (Stern & Kumar, 2017).

In this study, six aspects of PMT and information privacy concern were hypothesized. The following hypotheses are as follows, H1: Information privacy concern is significantly associated with privacy protection behaviour strategies, H2: Perceived severity is significantly associated with information privacy concern, H3: Perceived vulnerability is significantly associated with information privacy concern, H4: Self-efficacy is significantly associated with information privacy concern, H5: Response efficacy is significantly associated with information privacy concern and H6: Reward is significantly associated with information privacy concern. The proposed research model is presented in Figure 1.

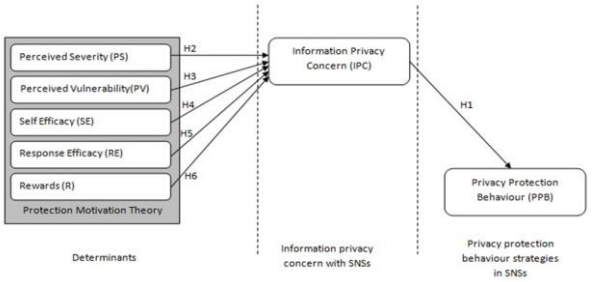

Figure 1: Proposed Research Model

4 Research Methodology

For the purpose of this study, a total of six hypotheses were tested and a quantitative approach was employed to them. Quantitative approach is the best method to use in order to test any existing theory as it involves a collection and statistical analysis of numerical data. (Ary, Jacobs, Razavieh, & Sorensen, 2010).

The instrument used in this study was a questionnaire that consisted of 44 items in total. All the items used a five point Likert scale, where 5 represented strongly agree and 1 represented strongly disagree.

4.1 Sample Selection and Data Collection

For the sampling process, stratified random sampling was used in this study. From the data given by the universities' administration on the number of active undergraduates as of February 26, 2015, there were approximately 9,205 undergraduates in total. As according to Sedek, Mahmud & Jalil (2012), they recommended that the ideal number for sample size suitable for analysis using SEM should be approximately between 300 to 800 samples. Of the 550 distributed, 499 were returned. 485 were usable for the purpose of this study with a response rate of 88%. Table 1 shows the profile of the respondents.

Variable	Type	Frequency	Percent
Gender	Male	2 5 4	5 2
	Female	2 3 1	4 8
Age	15-20	-	-
	21-25	449	93
	26-30	36	7
	31-35	-	-

5 Results

The first step conducted in SEM analysis was Confirmatory Factor Analysis (CFA). CFA was meant to identify the individual construct and was employed for three major purposes, which are (i) model fit, (ii) convergent validity and (iii) construct validity.

Maximum likelihood estimate (MLE) was used to estimate the structural model. Table 2 presents the test of overall model fit. All the fit indices were above recommended values.

Construct	Convergent Validity	
	(CR) (Above 0.6)	(AVE) (Above 0.5)
Privacy protection behaviour (PPB)	0.874	0.587
Information privacy concern (IPC)	0.917	0.650
Perceived severity (PS)	0.833	0.555
Perceived vulnerability (PV)	0.845	0.579

Self-efficacy (SE)	0.882	0.882
Response efficacy (RE)	0.867	0.623
Rewards (R)	0.903	0.702

Figure 2 presents the detailed result of the structural model. The R2 values for information privacy concern and privacy protection behaviour is 0.55 and 0.08 respectively. The root mean square error of approximation (RMSEA), which measures the discrepancy per degree of freedom, was 0.065. The goodness-of-fit index (GFI) was 0.851, comparative fit index (CFI) was 0.882 and the discrepancy Chi Square (Chisq/df) was 2.964.

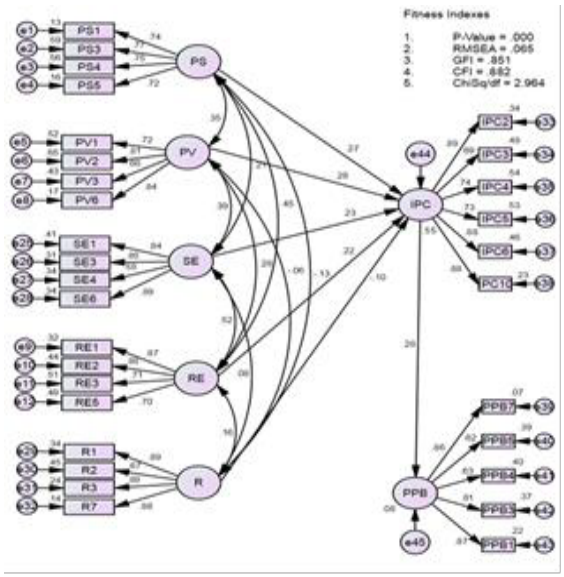

Figure 2: The Structural Model

Table 5: The regression path coefficients, significance values and hypothesis statement for every path and its conclusion

Source	Destination	Hypothesis Statement of Path Analysis	Estimates	P-value	Results on Hypothesis
IPC -->	PPB	H1.Higher information privacy concern will increase privacy protection behaviour.	0.28	0.003	Supported
PS -->	IPC	H2.Higher perceived severity will increase information privacy concern.	0.27	0.043	Supported
PV -->	IPC	H3.Higher perceived vulnerability will increase information privacy concern.	0.28	0.033	Supported
SE -->	IPC	H4.Higher self-efficacy will increase information privacy concern.	0.23	0.028	Supported
RE-->	IPC	H5.Higher response efficacy will increase information privacy concern.	0.22	0.001	Supported
R -->	IPC	H6. Higher rewards will reduce information privacy concern.	-0.10	0.605	Not Supported

6 Conclusion

The data analysis as executed from SEM reveals that there was a significant relationship of perceived severity, perceived vulnerability, response efficacy and self-efficacy towards information privacy concern as well as a significant relationship of information privacy concern and privacy protection behaviour strategies.

Similar with the results of prior research, individuals who are concerned with their information privacy in SNSs were found to use and adopt privacy protection behaviour strategies (Kim & Kim, 2016).). In order to materialise such concern and awareness, several determinants have been found. Perceived severity was found to be one such determinant. Users who feel that they will be seriously affected by the loss of information privacy will be more concerned with their information privacy, whereas those who think otherwise will not be as concerned. The next determinant that is significantly associated with information privacy concern is perceived vulnerability. The finding suggests that individuals who have been or are exposed to the loss of information privacy are more concerned with information privacy, whereas those who have not been or are not exposed to such a loss are less concerned. The next determinant proven in this study that contributes to information privacy concern is self-efficacy. Individuals who believe that they have the ability to use the protective strategies in SNSs will be more concerned with their information privacy. Finally, the last determinant that contributes to information privacy concern is response efficacy. One determinant however, was found does not support the hypotheses as stated in this study. It was found that reward is not significantly associated with information privacy concern.

References

1. Adhikari, K., & Panda, R. K. (2017). Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks: Evidence from India.
2. Ary, D., & Jacobs, L. C., Sorensen, C., & Razavieh, A.(2010). Introduction to research in education.
3. Boyd, D. (2008). Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence. Convergence: The International Journal of Research into New Media Technologies, 14(1):13–20.
4. Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. Computers in Human Behavior, 70, 291-302.
5. Compeau, D., Higgins, C. A., and Huff, S. (1999). Social cognitive theory and individual reactions to computing technology: A longitudinal study. MIS

Quarterly, 23(2):145–159.

6. Grindley, E. J., Zizzi, S. J., and Nasypany, A. M. (2008). Use of protectiomotivation theory, affect, and barriers to understand and predict adherence to outpatient rehabilitation. Physical Therapy. Jounal of American Physical Theraphy Association, 88(12):1529–1540.
7. Johnston, B. A. C. and Warkentin, M. (2010). Fear Appeals and Information security Behaviors: An Empirical Study. Ministry of Education Official Website, 34(3):549–566.
8. Kim, A. Y., & Kim, T. S. (2016). Factors Influencing the Intention to Adopt Identity Theft Protection Services: severity vs Vulnerability. In PACIS (p. 68).
9. Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, 64, 122-134.
10. MCMC (2014). Communications & Multimedia Pocket Book of Statistic.
11. Marett, K., McNab, A. L., & Harris, R. B. (2011). Social networking websites and posting personal information: An evaluation of protection motivation theory. AIS Transactions on Human-Computer Interaction, 3(3), 170-188.
12. Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. Journal of Marketing, 81(1), 36-58.
13. Nemec Zlatolas, L., Welzer, T., Heri˘cko, M., and H¨olbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. Computers in Human Behavior, 45:158–167.
14. Palladino, B. E., Menesini, E., Nocentini, A., Luik, P., Naruskov, K., Ucanok, Z., ... & Scheithauer, H. (2017). Perceived Severity of Cyberbullying: Differences and Similarities across Four Countries. Frontiers in Psychology, 8, 1524.
15. Salleh, N., Hussein, R., Mohamed, N., Abdul, N. S., Ahlan, A. R., and Aditiawarman, U. (2012). Examining Information Disclosure Behavior on Social Network Sites Using Protection Motivation Theory, Trust and Risk. Journal of Internet Social Networking & Virtual Communities, 2012.
16. Schoeman, F. (1984). Philosophical Dimensions of Privacy: An Anthology.
17. Sedek, M., Mahmud, R., Jalil, H. A., & Daud, S. M. (2012). Types and levels of ubiquitous technology use among ICT undergraduates. Procedia-Social and Behavioral Sciences, 64, 255-264.
18. Stern, T., & Kumar, N. (2017). Examining privacy settings on online social networks: a protection motivation perspective. International Journal of Electronic Business, 13(2-3), 244-272.
19. Vithessonthi, C. (2010). Knowledge sharing, social networks and organizational transformation. The Business Review, Cambridge, 15(2):99–109
20. Warren, S. D. and Brandeis, L. D. (1890). The Right to Privacy. Harvard Law Review, 4(5):193–220.