International Business Management 10 (16): 3682-3691, 2016
ISSN: 1993-5250
© Medwell Journals, 2016

Factors of Concerning Privacy-Protection Social Networking Sites

[1]Nur Fadzilah Othman, [1]Rabiah Ahmad and [2]Muliati Sedek
[1]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, Malaysia
[2]Center for Teaching and Learning, Universiti Teknikal Melaka,
76100 Durian Tunggal, Melaka, Malaysia

Abstract: This study attempts to gain an insights in identifying factors of information privacy concern and protection behaviour as well as it factors in using social networking sites. The factors are gathered from the protection motivation theory, hyper-personal framework and privacy protection behaviour. Thus, this study explains the roles of information privacy concerns in social networking sites by investigating the cause as well as behavioural strategies that individual utilize in protecting their privacy. An empirical analysis involved a total of 488 undergraduates students from a public Malaysian university. Data was analyzed using a Structural Equation Modelling (SEM) technique and results were based on the SEM outputs which demonstrate the acceptance and confirmation of all factors. Results indicates that information privacy concern among user contribute to privacy protection behaviour. Perceived severity, perceived vulnerability, rewards, perceived anonymity of others and perceived intrusiveness are found to be the factors for information privacy concern.

Key words: Social networking sites, information privacy concern, privacy protection behaviour, protection motivation theory, hyperpersonal framework

INTRODUCTION

Social Networking Sites (SNSs) have become an obsession among Malaysian. Statistics demonstrated that total of 13.3 million users or 45.5% of the population were registered as Facebook user (MCMC, 2014). This is due to the features of SNSs that offer user to create public or semi-public profiles, connect with other users and view lists of connections of their connection (Boyd and Ellison, 2007). Services provided by SNSs also enabling user to own public profiles opened or closed, interact with other user and see activities done by their friends and strangers depending on the openness of the user's profile.

The popularity of SNSs attracted researchers from various disciplines including technology, communication and sociology (Zlatolas *et al*., 2015). Privacy issues is one of the hottest topic among all the concerns in SNSs because of the characteristic of SNSs which involving large number of users and the huge pile of unprotected information about them, shared with known and unknown person with minimum restrictions. Openness nature in SNSs allow information seeker to gain any information provided by user without realizing that such information may be misused by unscrupulous individuals. Although, SNSs itself have been equipped with systematic safety features but it cannot be guarantee that one's privacy is fully protected (Salleh *et al*., 2012). Therefore, user need an assessment's mechanism of threats and benefits from engaging in risky situation in order for them to determine how much and what type of personal information can be disclosed.

This study aims to investigate factors contribute user's privacy protection behaviour in SNSs. Understanding the factors of privacy protection behaviour of SNSs can create awareness among user to protect themselves and develop the ability and confidence in impose their self-control through the implementation of privacy protection behaviour in SNSs.

Information privacy concern and privacy protection behaviour: The concept of privacy based on Westin (1970) is that privacy is one's control over his or her own personal information. Westin (1970) defined privacy as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others".

Correspoding Author: Nur Fadzilah Othman, 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, Malaysia

The definition of information privacy is the "ability of an individual to personally control information about one's self" whereas information privacy concern are the "extent to which an individual is concerned about organizational practices related to the collection and use of his or her personal information (Smith *et al.*, 1996). Several research has been done and posits that information privacy concern had an impact to protection behaviour (Feng and Xie, 2014; Jiang *et al.*, 2013; Mohamed and Ahmad, 2012; Youn, 2009). Since, online companies depend on the ability to collect large amounts of personal information about users, information privacy is a critical ethical issue in online environments (Son and Kim, 2008). Users with high privacy concern will adopt several privacy strategies to protect their privacy from e-Marketers (Youn, 2009). Hence, it would be interesting to investigate factors contribute to information privacy concern and consequently encourage user to practice privacy protection behaviour in SNSs.

Individuals behaviour concern has crucial role in development of SNSs (Dhawan and Goel, 2014). Although, the privacy concerns of users are significant but their attitude towards the risks of personal information disclosure is still very relaxed. Dhawan and Goel (2014). SNSs have been provided with privacy measures and it all depends on users either they want to use them or leave them with default setting. Users who are unaware of privacy issue in SNSs may be leave the privacy setting in default mode. In other words, it is assume that, individuals will likely use privacy settings provided by SNSs to protect their privacy if they have higher concerns with their information privacy.

Theoretical framework and hypotheses

Protection motivation theory: Protection Motivation Theory (PMT) developed by Rogers (1975) postulates that individual's motivation to protect one from risks comes from: perceived severity, perceived vulnerability and response efficacy. The model was modified to explain failure involved in protection behaviour by including, self-efficacy, response cost and rewards associated with risky behaviour (Rogers, 1983, 1975). The theory has been primarily used in health industry literature (Fruin *et al.*, 1992; Floyd *et al.*, 2000) and according to Grindley *et al.* (2008), PMT is one such preventative health behavior theory that has been used in >20 different health-related fields to study intentions and behavior. PMT also has been widely used in Information System (IS) field to examine protection behaviour in online transaction (Youn, 2009; Lee *et al.*, 2008), awareness of employees in organizational information security policy (Vance *et al.*, 2012) and individual use of security software (Johnston and Warkentin, 2010).

Perceived severity: Perceived severity explains the judgement of the severity significance resulting from a threatening security event (Lee *et al.*, 2008). Perceived severity assesses how severe an individual believes a threat will be to their life. The more seriously a person perceives the negative consequence, the more he or she will adopt recommended actions (Zhang and McDowell, 2009). Online consumers will more likely adopt protection when they faces greater perceived severity and seriousness of the threat (Lee *et al.*, 2008). This is also supported by Youn (2009), claims that an individual's motivation for engaging in risk-reducing behaviour is increased by perceived severity. Nevertheless, this is contrary to the studycarriedout by Zhang and McDowell (2009), identifies that perceived severity is not a determinant of password protection intention for online users. Users will develop a perceived severity after losing information privacy in SNSs and they are more likely concern with information privacy. So, the research proposes that individuals who perceive severe consequences have higher concerns with their information privacy in SNSs.

Perceived vulnerability: Perceived vulnerability refers to individual's perception of experiencing possible negative effect stemming from performing risky behaviour while Lee *et al.* (2008), justified perceived vulnerability is the degree to which an individual believes a threat will occur to him/her. Several studies supports that perceived vulnerability positively impacting individual protection behaviour. Perceived severity found to increase students' intention to perform malware avoidance behaviour (Fuller *et al.*, 2014) and also a major antecedents to privacy concern when using an internet (Dinev and Hart, 2004). Similarly, Mohamed and Ahmad (2012), agreed that perceived vulnerability are one of the factor contributing to information privacy concern in SNSs. Conversely, perceived vulnerability had an n insignificant impact on employees' intention to comply with IS security policies (Vance *et al.*, 2012). Thus, the research suggests that individuals who perceive the risk and threats of losing information privacy through SNSs have big concerns with their information privacy.

Response efficacy: Response efficacy is the belief that a proposed countermeasure will be successful in avoiding the threat (McClendon and Prentice-Dunn, 2001) and individual's confidence that recommended behaviour will prevent them from threat. Research suggests that response efficacy is significant predictor behaviour in determining the decision of home wireless network users to implement security features on their networks (Woon *et al.*, 2005), influences behaviour intention to use anti-spyware software as a protective technology (Chenoweth *et al*., 2009), predicts backing up data on personal computers (Crossler, 2010) and increases intention to perform malware avoidance behaviours when using personal mobile devices (Dang-pham and Pittayachawan, 2015). Hence, the research posits that individuals who believe that protective action in SNSs can avoid them in losing information privacy is more likely to be concerned with their information privacy.

Self-efficacy: Self-efficacy can be define as individua's belief that they have capability to implement the protective behaviour. Self-efficacy plays an important role in user's choice to perform risky online behaviour (Milne *et al*., 2009). Some studies provide evidence for positive relationship between self-efficacy and motivation to protect information online. Vance *et al*. (2012), found that the employees' belief that they can successfully comply with security policies and enhance compliance with policies and procedures. Furthermore, research done by Lee *et al*. (2008), proves that self-efficacy should be influential factors of stimulation to perform a protection behaviour. Self-efficacy have an influence on individual concerns for information privacy (Korzaan and Boswell, 2008) and determinant on trust and utilization of decision support system (Madhavan and Phillips, 2010). Nevertheless, other studies found that self-efficacy did not related to privacy concern (Youn, 2009) and no relationship with information personal information disclosure (LaRose and Rifon, 2007). Therefore, this research assume that individuals with high self efficacious in using SNSs are more likely to be concern with their information privacy.

Rewards: Rewards refer to individual's expectation in getting benefits when keeping with the selecting behaviour (Lee *et al*., 2008). Rewards give significant negative influence on intention and suggesting that individuals who find great enjoyment and satisfaction from sharing personal information are less inclined to make the adaptive change for protection (Marett *et al*., 2011). The higher the rewards attained by not taking a recommended protective action, the less likely the individual is to take that action (Milne *et al*., 2002). SNSs ask for personal information such as name, photo, email, address and telephone number in exchange for rewards. Individuals who do not want to expose and disclose their personal information may not vulnerable to information security problems including viruses, privacy intrusion and identity theft. Additionally, individuals that willing to disclose their information may experience sense of being close to their friends and family (Baren *et al*., 2003) and getting satisfaction from togetherness feeling (Ijsselsteijn *et al*., 2009). Individuals may expose their personal information in order to getting connected to others or playing games in SNSs. So, this research asserts that individuals who perceive great rewards by using SNSs have less concern with their information privacy.

Hyperpersonal framework: Hyperpersonal framework suggested by Walther (1996), offers an approach to understand how user experience relational intimacy in mediated communication medium. Hyperpersonal framework consists of four elements of mediated communication which show how senders select, receivers magnify, channels promote and feedback facilitate development of social relationships in the mediated environment (Jiang *et al*., 2013). Several study used hyperpersonal framework to comprehend the relationship development in mediated environment. Yao and Flanagin (2006), explain the effect of self-awareness from the perspective of sender towards individuals' social attractiveness in instant messaging whereas the receiver perspective explain on impressions management in teleconferencing (Walther, 2007). In order to shape self-presentation behaviour in online dating websites, channel characteristic and feedback are the essential element (Gibbs *et al*., 2011).

Perceived anonymity of self: Based on hyperpersonal framework, sender perspective consider as an consequences of limited identity cues on individuals' impression management and individuals will focus on the information they have selectively sent to other (Jiang *et al*., 2013). Perceived anonymity of self was examined to reflect the sender perspective. Findings shows that higher perceived anonymity of self will reduce individuals' information privacy concern in online chat room (Jiang *et al*., 2013). Individuals will feel responsible while going online if they feel there is someone else knows their personal information (Ji and Lieber, 2010). Hence, if the individuals perceived themselves unidentifiable or anonymity in SNSs, they feel secured and protected against others scrutiny and attention. So, it will cause them less concerned about their information privacy.

Perceived anonymity of others: Hyperpersonal framework suggest that limited identity cues also play an important key in establishing the receiver perspective. Because of lack physical appearance in online social interaction, the other person identity can often be partial or fragmented and others can at times remain largely unidentifiable (Jiang *et al*., 2013). With regard to Viegas (2005),

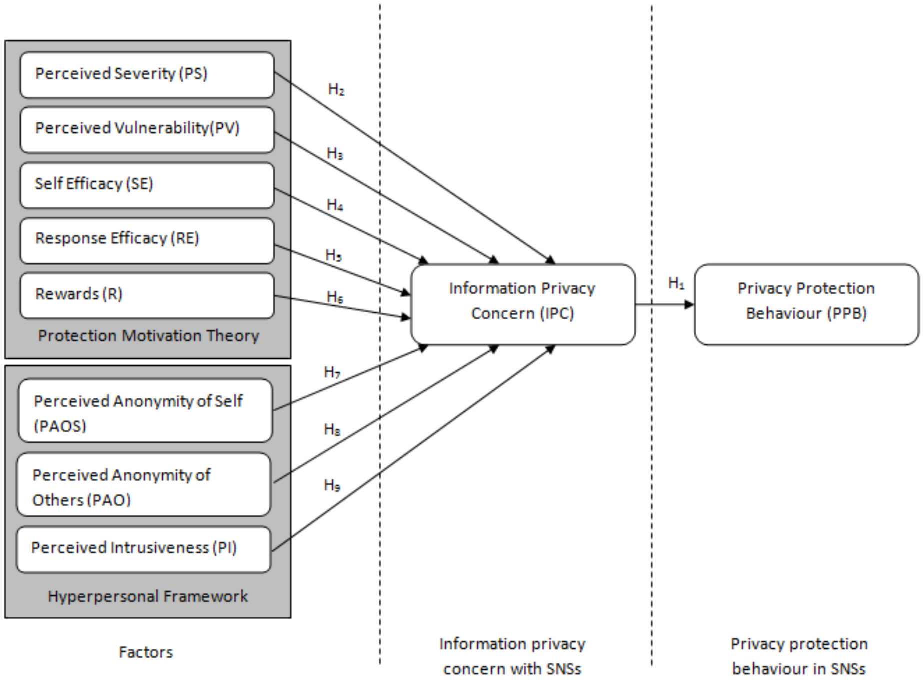
Perceived Severity (PS)
Perceived Vulnerability(PV)
Self Efficacy (SE)
Response Efficacy (RE)
Rewards (R)
Protection Motivation Theory
Perceived Anonymity of Self (PAOS)
Perceived Anonymity of Others (PAO)
Perceived Intrusiveness (PI)
Hyperpersonal Framework
H_2
H_3
H_4
H_5
H_6
H_7
H_8
H_9
Information Privacy Concern (IPC)
H_1
Privacy Protection Behaviour (PPB)
Factors
Information privacy concern with SNSs
Privacy protection behaviour in SNSs

Fig. 1: Research model

individuals feel anxious and paranoid about losing their privacy if they fail to know much about other pasties in social interactions. Besides, past studies also suggest that when others provide adequate explanations, individuals will become more acceptable and tolerant towards privacy loss (Colquitt, 2001). Perceived anonymity of others reflect receiver perspective in this research as the unidentifiable or anonymity of others in SNSs will increase individual's information privacy concern.

Perceived intrusiveness: To establish understanding of others, individuals will interpret other's feedback in social interaction (Walther, 1996). In online interaction, feedback occurs of in the way personal information is exchanged and others ask questions or provide answers in a to-and-fro manner (Jiang *et al*., 2013). Individuals typically maintain psychological boundary to control access to their private self during exchanging information (Petronio, 2002). Psychological boundaries can be break if people disclose personal informationin response to requests from others. It might awaken individuals' perceived in trusiveness because of psychological boundaries penetrations (Vandebosch and van Cleemput, 2009). In this research it posit that higher perceived intrusiveness will increase information privacy concern in SNSs.

By integrating protection motivation theory and hyperpersonal framework, proposed research model presented in Fig. 1. In this study, we hypothesize five aspects of PMT, three aspects of hyperpesonal framework and information privacy concern. We also propose investigating the effects of information privacy concern on privacy protection behaviour. The following hypotheses as follows:

- H_1: higher information privacy concern will increase privacy protection behaviour
- H_2: higher perceived severity will increase information privacy concern
- H_3: higher perceived vulnerability will increase information privacy concern
- H_4: higher self-efficacy will increase information privacy concern
- H_5: higher response efficacy will increase information privacy concern
- H_6: higher rewards will reduce information privacy concern
- H_7: higher perceived anonymity of self will reduce information privacy concern
- H_8: higher perceived anonymity of others will increase information privacy concern
- H_9: higher perceived intrusiveness will increase information privacy concern

Because existing theories and empirical evidence do not hint at a clear causal relationship between response cost in protection motivation theory and channel element in hyperpersonal framework towards information privacy concern, we do not hypothesize on them.

MATERIALS AND METHODS

For the purpose of this study, a total of nine hypotheses were tested. Therefore, a quantitative approach was employed to test the hypotheses. This is based on Ary *et al.* (2010); the best method to use in order to test any existing theories and it involves a collection and statistical analysis of numerical data is quantitative approach. Instrument used in this study was a questionnaire that consisted of 59 items in total. Five items for perceived severity adapted from Crossler (2010), LaRose and Rifon (2007) and Woon *et al.* (2005). Six items for perceived vulnerability adapted from Woon *et al.* (2005) and Dinev and Hart (2004). Five items for self-efficacy were adapted from Crossler (2010), LaRose and Rifon (2007) and Woon *et al.* (2005). Five items for response efficacy adapted from Crossler (2010), Zhang and McDowell (2009) and Lee *et al.* (2008) while six items for rewards were adapted from Youn (2005). The 4 items for perceived anonymity of self and 4 items for perceived anonymity of others adapted from (Pinsonneault and Heppel, 1997), 6 items for perceived intrusiveness adapted from (Burgoon *et al.*, 1989), 10 items for information privacy concern adapted from (Dinev and Hart, 2004). Finally 7 items for privacy protection behaviour were adapted from (Feng and Xie, 2014). All the item were using a 5 point Likert scale and where 5 represented strongly agree and 1 represent strongly disagree responses.

The items for this instrument was validated by group of experts from other public university and Cyber Security Malaysia (CSM). Then, we pilot the instrument to 40 samples. Next, the collected data was analysed using SPSS to determine its validity. Final version of questionnaires consists of 43 items from 59 items. AMOS programme has been used to analysed the data and to confirm selected item for each construct hence validate the framework.

Sample selection and data collection: Stratified random sampling used for sampling process. 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. Sedek, Mahmud recommended that the ideal number for sample size suitable for analysis using SEM should approximately be between 300-800 samples. Of 550 distributed, 503 were returned. The 488 were usable for the purpose of this study, a response rate of 89%. Table 1 shows the profile of respondents.

Table 1: Profile of respondent

Variable/type	Frequency	Percent
Gender		
Male	256	52
Female	232	48
Age		
15-20	-	-
21-25	452	93
26-30	36	7
31-35	-	-

RESULTS AND DISCUSSION

The first step conducted in SEM analysis is Confirmatory Factor Analysis (CFA) (Hair *et al.*, 2010). CFA was meant to identify the individual construct and employed for three major purpose, namely to test for model fit, convergent validity and construct validity.

Maximum Likelihood Estimate (MLE) used to estimate the structural model. Table 2 presented the test of overall model fit. All the fit indices were above recommended value. As shown in Table 3 is the set of criteria for fit indices and their recommended value. Table 4 shows the result of fitness indexes for research model. All required level was is achieved.

The Root Mean Square Error of Approximation (RMSEA) which measure the discrepancy per degree of freedom was 0.056, the Goodness-of-Fit Index (GFI) was 0.831, Comparative Fit Index (CFI) was 0.883 and discrepancy Chi-square (Chi-square/df) was 2.472.

Figure 2 presents the detailed result of the structural model. The R^2 values 0.13 for information privacy concern and 0.03 for privacy protection behaviour. As shown in Fig. 1, path from self-efficacy to information privacy concern, response efficacy to information privacy concern and perceived anonymity of self were insignificant whereas all the other paths were significant. Thus, H_4, H_5 and H_7 are not supported while H_1, H_2, H_3, H_6, H_8 and H_9 are supported. The summarize of regression path coefficients, significance value and hypothesis statement for every path and its conclusion shows in Table 5.

Overall, this study has advanced the understanding in information privacy concern, its factors and privacy protection behaviour in SNSs in the Malaysian context. Findings from this study shows an evidence that user in SNSs will used privacy protection strategies in SNSs if they concerned with their information privacy. The research had identified eight factors contribute to information privacy concern in SNSs. But out of eight, only five appeared as significant factors to information privacy concern. Perceived severity, perceived vulnerability, rewards, perceived anonymity of others and perceived intrusiveness found to be a factors to information privacy concern Appendix A.

The first factor proven in this study as a factor of information privacy concern is perceived severity. Individuals who perceived the severity of losing personal information such as photos and identity stolen have high concern towards their information privacy and accordingly they will adopt privacy protection behaviour in SNSs. It supports by previous research done by

Table 2: Result of CFA for measurement model

	Convergent validity	
Construct	Composite Reliability (CR) (above 0.6)	Average Variance Extracted (AVE) (above 0.5)
Privacy protection behaviour	0.976	0.874
Information privacy concern	1.181	3.571
Perceived severity	1.215	2.735
Perceived vulnerability	1.173	2.288
Self-efficacy	0.963	0.868
Response efficacy	0.919	0.743
Rewards	1.171	2.223
Perceived anonymity of self	0.862	0.654
Perceived anonymity of others	1.187	2.501
Perceived intrusiveness	0.908	0.721

Table 3: Categories of model fit and their level of acceptance

Name of category	Name of index	Level of acceptance	Sources
Absolute fit	RMSEA	≤0.08	Awang
Incremental fit	GFI	≥0.80	Baumgartner and Homburg (1996), Doll *et al.* (1994)
	CFI	≥0.80	Baumgartner and Homburg (1996), Doll *et al.*, 1994)
Parsimonious fit	Chi-square/df	≤3.00	Awang

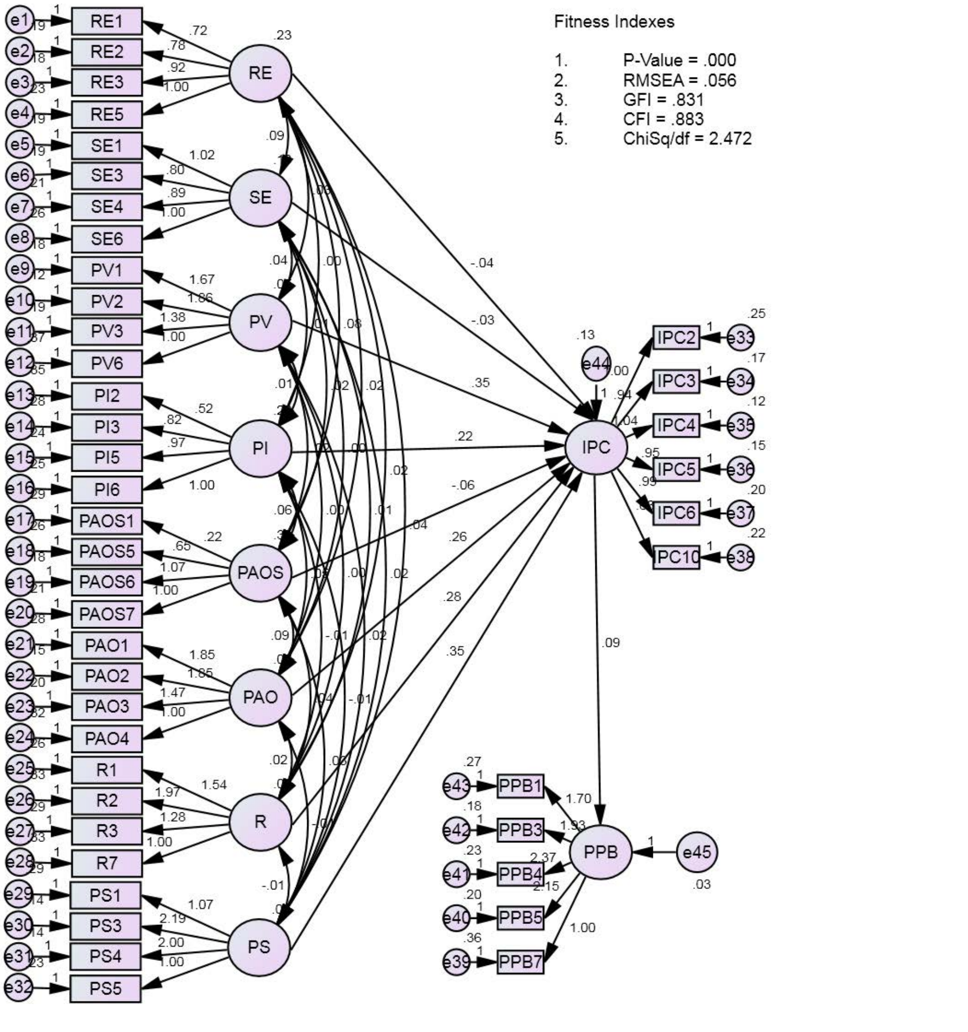

Fig. 2: The structural model

Table 4: The fitness Indexes for research model

Name of category	Name of index	Index value	Comments
Absolute fit	RMSEA	0.056	The required level is achieved
Incremental fit	GFI	0.831	The required level is achieved
	CFI	0.883	The required level is achieved
Parsimonious fit	Chisq/df	2.472	The required level is achieved

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

Source	Destination	Hypothesis statement of path analysis	Estimates	p-values	Results on hypothesis
IPC-->	PPB	H_1: Higher information privacy concern will increase privacy protection behaviour	0.09	0.003	Supported
PS-->	IPC	H_2: Higher perceived severity will increase information privacy concern	0.35	0.043	Supported
PV-->	IPC	H_3: Higher perceived vulnerability will increase information privacy concern	0.35	0.001	Supported
SE-->	IPC	H_4: Higher self-efficacy will increase information privacy concern	-0.03	0.698	Not supported
RE-->	IPC	H_5: Higher response efficacy will increase information privacy concern	-0.04	0.605	Not supported
R-->	IPC	H_6: Higher rewards will reduce information privacy concern	0.28	0.028	Supported
PAOS-->	IPC	H_7: Higher perceived anonymity of self will reduce information privacy concern	-0.06	0.293	Not supported
PAO-->	IPC	H_8: Higher perceived anonymity of others will increase information privacy concern	0.26	0.033	Supported
PI-->	IPC	H_9: Higher perceived intrusiveness will increase information privacy concern	0.22	0.001	Supported

Mohamed and Ahmad (2012) and Chenoweth *et al.* (2009). Second factor is perceived vulnerability. Individuals who believe that risk and threat they faced in SNSs will makes them more concern towards their information privacy. This findings is in line with previous researchers on user's information disclosure in social media (Salleh *et al.*, 2012) and user's expectation of online scams (Crossler, 2010). Next factors is rewards that also supported by past studies. Based on the findings by Youn (2009) and Salleh *et al.* (2012) proves that great rewards gain from online activity make them less concern with their information privacy. Fourth factor is perceived anonymity of others. Users of SNSs more concerns with their information privacy and accordingly adopt privacy protection behaviour. Past studies that support this research done by Jiang *et al.* (2013) found that perceived anonymity of others affect privacy concern in online chat. Finally, the last factor contribute to information privacy concern is perceived intrusiveness. Supported by prior research done by Jiang *et al.* (2013), individuals that feel disturbed in SNSs will increase their information privacy concern, thus will perform privacy protection behaviour.

Conversely, there is three factors found do not support the hypotheses stated in this study namely self-efficacy, response efficacy and perceived anonymity of self. First factor is self-efficacy which states that higher self-efficacy will increase information privacy concern. In this study it is found that user with higher self efficacy lead to low information privacy concern. It is support from research done by Youn (2009). This is perhaps because users feel that they can strongly control their information privacy and have little concern about negative effect when sharing their personal information in SNS. As a result, their self efficacy may not lead to motivation to protect privacy. Another factor is response efficacy. Finding in this study is similar with Mohamed and Ahmad (2012) that argues response efficacy will not increase information privacy concern. A plausible explanation is users giving full confidence that privacy settings provided by SNSs provider can protect their information and make them feel safe to disclose their information and less concern towards information privacy. Although, SNSs have been provided with privacy settings and privacy policies to control and customize the information shared with other users, unfortunately it shows that it is not enough to protect one's sensitive data (Zheleva and Getoor, 2009). Finally, the last factor which does not support the hypotheses stated in this study is perceived anonymity of self derives from hyper personal framework. Results in this study conclude that individuals perceived themselves unidentifiable or anonymity in SNSs will increase their information privacy concern.

CONCLUSION

Finally, this research is very valuable in providing guidelines for SNSs user to behave properly to ensure their privacy is protected. It is important for the user to know the appropriate protection behaviour in dealing with privacy and make SNSs is a safer place.

Appendix A: survey items in final data analysis

Information privacy concern:

- I am concerned about the potential misuse of my personal data in SNSs
- I am concerned that my personal information has not been stored safely
- I am concerned that SNSs would sell my personal information in their database to other companies
- I am concerned that I lost control over my personal information in SNSs
- I am concerned that SNSs would share my personal information without permission
- I am concerned about providing personal information in SNSs, because of what others might do with it

Perceived severity:

- I believe that by losing information privacy through SNSs would be a serious problem for me
- I believe that by having my identity stolen through SNSs would be a serious problem for me
- I believe that by revealing about my feeling and emotion through SNSs would involve mny unexpected problems
- In general, it is risky to reveal my personal information on SNSs

Perceived vulnerability:

- I feel that my personal information in SNSs could be misused
- I feel that my personal information in SNSs could be made available to unknown individuals or companies without my knowledge
- I feel that my status updates in SNSs could be inappropriately used
- I can faced to an information security problems (e.g., virus, privacy, identity theft, hacking and etc.) in SNSs

Self-efficacy:

- I believe that I have the ability to protect my personal information in SNSs
- I believe that it is easy for me to enable privacy measure features on SNSs by myself
- I believe that I can comply with privacy policy provided by SNSs by myself
- I feel confident in my acquired skills to protect my privacy on the SNSs

Response efficacy:

- I could probably protect myself from losing my information privacy, if I used privacy protection measures in SNSs
- I could probably protect my information privacy better if I use privacy protection measures in SNSs
- I could probably prevent other user from stealing my personal information, if I used privacy protection measures in SNSs
- I could probably protect me from online dangers, if I used privacy protection measures in SNSs

Rewards:

- I could get connected with new friends and friends from the past by sharing my information privacy in SNSs
- I think that by sharing my profile with others is quite enjoyable
- I feel that by sharing my profile with others improve my reputation
- I earn respect from others by sharing my profile with them

Perceived anonymity of self:

- I believe the other user in SNSs know about me
- I believe that if I use nickname, it was impossible for anyone to identify me in SNSs
- I believe that if I didnot use actual picture for my profile picture , it was impossible for anyone to identify me in SNSs
- I believe that if I did not specify my personal information, it was impossible for anyone to identify me in SNSs

Perceived anonymity of others:

- I believe that I know about the other user in SNSs
- I believe that if other users use nickname, it was impossible for me to identify them in SNSs
- I believe that if other users did not use actual picture for their profile picture , it was impossible for me to identify them in SNSs
- I believe that if other user did not specify their personal information, it was impossible for me to identify them in SNSs

Perceived intrusiveness:

- I feel that other user in SNSs was intrusive
- I feel that other users did not respect my need for personal space in SNSs
- I feel that other users was harassing me during the interaction in SNSs
- I feel that my privacy in SNSs was disturbed

Privacy protection behaviour:

- I would consider making up fabricated responses to avoid giving the SNSs real information about myself
- I would only fill up data partially when registering with SNSs
- I would set my SNS profile visibility to protect my privacy in SNSs
- I would refer relevant guidelines for example from Cyber Security Malaysia website deal with SNSs
- I would delete or deactivate my profile or account

ACKNOWLEDGEMENTS

Researchers are grateful to Universiti Teknikal Malaysia Melaka (UTeM) for the financial support through grant scheme (FRGS/2/2013/ICT07/UTEM/02/1) and Ministry of Higher Education of Malaysia for the financial support through the fellowship scheme.

REFERENCES

Ary, D., L.C. Jacobs, A. Razavieh and C.K. Sorensen, 2010. Introduction to Research in Education. 8th Edn., Cengage Learning, Belmont, CA., USA., ISBN-13: 978-0495601227, Pages: 696.

Baren, J., W. Ijsselsteijn, N. Romero, P. Markopoulos and B. de Ruyter, 2003. Affective benefits in communication: The development and field-testing of a new questionnaire measure. Proceedings of the 6th Annual International Workshop on Presence, October 6-8, 2003, Aalborg, Denmark, pp: 1-5.

Baumgartner, H. and C. Homburg, 1996. Application of structural equation modeling in marketing and consumer research: A review. Int. J. Res. Market., 13: 139-161.

Burgoon, J.K., R. Parrott, B.A. Le Poire, D.L. Kelley, J.B. Walther and D. Perry, 1989. Maintaining and restoring privacy through communication in different types of relationships. J. Social Personal Relationships, 6: 131-158.

Chenoweth, T., R. Minch and T. Gattiker, 2009. Application of protection motivation theory to adoption of protective technologies. Proceedings of the 42nd Hawaii International Conference on System Sciences, January 5-8, 2009, Big Island, HI., USA., pp: 1-10.

Colquitt, J.A., 2001. On the dimensionality of organizational justice: A construct validation of a measure. J. Applied Psychol., 86: 386-400.

Crossler, R.E., 2010. Protection motivation theory: Understanding determinants to backing up personal data. Proceedings of the 43rd Hawaii International Conference on System Sciences, January 5-8, 2010, Honolulu, HI., USA., pp: 1-10.

Dang-Pham, D. and S. Pittayachawan, 2015. Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A protection motivation theory approach. Comput. Secur., 48: 281-297.

Dhawan, S. and S. Goel, 2014. Analysis of pattern of information revelation and site use behavior in social networking sites. Int. J. Comput. Applic. Technol. Res., 3: 42-44.

Dinev, T. and P. Hart, 2004. Internet privacy concerns and their antecedents-measurement validity and a regression model. Behav. Inform. Technol., 23: 413-422.

Doll, W.J., W. Xia and G. Torkzadeh, 1994. A confirmatory factor analysis of the end-user computing satisfaction instrument. MIS Q., 18: 453-461.

Feng, Y. and W. Xie, 2014. Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. Comput. Hum. Behav., 33: 153-162.

Floyd, D.L., S. Prentice-Dunn and R.W. Rogers, 2000. A meta-analysis of research on protection motivation theory. J. Applied Social Psychol., 30: 407-429.

Fruin, D.J., C. Pratt and N. Owen, 1992. Protection motivation theory and adolescents' perceptions of exercise. J. Applied Social Psychol., 22: 55-69.

Fuller, B.T., S.M. Fahrni, J.M. Harris, A.B. Farrell and J.B. Coltrain *et al*., 2014. Ultrafiltration for asphalt removal from bone collagen for radiocarbon dating and isotopic analysis of Pleistocene fauna at the tar pits of Rancho La Brea, Los Angeles, California. Quaternary Geochronol., 22: 85-98.

Gibbs, J.L., N.B. Ellison and C.H. Lai, 2011. First comes love, then comes google: An investigation of uncertainty reduction strategies and self-disclosure in online dating. Commun. Res., 38: 70-100.

Grindley, E.J., S.J. Zizzi and A.M. Nasypany, 2008. Use of protection motivation theory, affect and barriers to understand and predict adherence to outpatient rehabilitation. Phys. Therapy, 88: 1529-1540.

Hair, Jr. J.F., W.C. Black, B.J. Babin and R.E. Anderson, 2010. Multivariate Data Analysis. 7th Edn., Prentice Hall, Upper Saddle River, NJ., ISBN-13: 9780138132637, Pages: 785.

Ijsselsteijn, W., J. van Baren, P. Markopoulos, N. Romero and B. de Ruyter, 2009. Measuring Affective Benefits and Costs of Mediated Awareness: Development and Validation of the ABC-Questionnaire. In: Awareness Systems: Advances in Theory, Methodology and Design, Markopoulos, P., B. de Ruyter and W. Mackay (Eds.). Chapter 20, Springer, London, UK., ISBN: 978-1-84882-476-8, pp: 473-488.

Ji, P. and P.S. Lieber, 2010. Am I safe? Exploring relationships between primary territories and online privacy. J. Internet Commerce, 9: 3-22.

Jiang, Z., C.S. Heng and B.C. Choi, 2013. Privacy concerns and privacy-protective behavior in synchronous online social interactions. Inform. Syst. Res., 24: 579-595.

Johnston, A.C. and M. Warkentin, 2010. Fear appeals and information security behaviors: An empirical study. MIS Q., 34: 549-566.

Korzaan, M.L. and K.T. Boswell, 2008. The influence of personality traits and information privacy concerns on behavioral intentions. J. Comput. Inf. Syst., 48: 15-24.

LaRose, R. and N.J. Rifon, 2007. Promoting *i*-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. J. Consum. Affairs, 41: 127-149.

Lee, D., R. LaRose and N. Rifon, 2008. Keeping our network safe: A model of online protection behaviour. Behav. Inform. Technol., 27: 445-454.

MCMC., 2014. Industry performance report 2013. Malaysian Communication and Multimedia Commision (MCMC), Malaysia. http://www.skmm.gov.my/skmmgovmy/media/General/pdf/IPR2013_English.pdf.

Madhavan, P. and R.R. Phillips, 2010. Effects of computer self-efficacy and system reliability on user interaction with decision support systems. Comput. Hum. Behav., 26: 199-204.

Marett, K., A.L. McNab and R.B. Harris, 2011. Social networking websites and posting personal information: An evaluation of protection motivation theory. AIS Trans. Hum.-Comput. Interact., 3: 170-188.

McClendon, B.T. and S. Prentice-Dunn, 2001. Reducing skin cancer risk: An intervention based on protection motivation theory. J. Health Psychol., 6: 321-328.

Milne, G.R., L.I. Labrecque and C. Cromer, 2009. Toward an understanding of the online consumer's risky behavior and protection practices. J. Consum. Affairs, 43: 449-473.

Milne, S., S. Orbell and P. Sheeran, 2002. Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. Br. J. Health Psychol., 7: 163-184.

Mohamed, N. and I.H. Ahmad, 2012. Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. Comput. Hum. Behav., 28: 2366-2375.

Petronio, S., 2002. Communication Privacy Management Theory. In: Boundaries of Privacy: Dialectics of Disclosure, Petronio, S. (Ed.). State University of New York Press, USA., ISBN-13: 9780791455159, pp: 168-180.

Pinsonneault, A. and N. Heppel, 1997. Anonymity in group support systems research: A new conceptualization, measure and contingency framework. J. Manage. Inform. Syst., 14: 89-108.

Rogers, R.W., 1975. A protection motivation theory of fear appeals and attitude change1. J. Psychol., 91: 93-114.

Rogers, R.W., 1983. Cognitive and Physiological Process in fear Appeals and Attitude Change: A Revised Theory of Protection Motivation. In: Social Psychophysiology: A Sourcebook, Cacioppo, J.T. and R.E. Petty (Eds.). Guildford Press, London, UK., ISBN-13: 9780898626261, pp: 153-176.

Salleh, N., R. Hussein, N. Mohamed, N.S.A. Karim, A.R. Ahlan and U. Aditiawarman, 2012. Examining information disclosure behavior on social network sites using protection motivation theory, trust and risk. J. Internet Social Networking Virtual Commun. 10.5171/2012.281869.

Smith, H.J., S.J. Milberg and S. Burke, 1996. Information privacy: Measuring individuals' concerns about organizational practices. MIS Quarterly, 20: 167-196.

Son, J.Y. and S.S. Kim, 2008. Internet users' information privacy-protective responses: A taxonomy and a nomological model. MIS Quart., 32: 503-529.

Vance, A., M. Siponen and S. Pahnila, 2012. Motivating IS security compliance: Insights from habit and protection motivation theory. Inform. Manage., 49: 190-198.

Vandebosch, H. and K. van Cleemput, 2009. Cyberbullying among youngsters: Profiles of bullies and victims. New Media Soc., 11: 1349-1371.

Viegas, F.B., 2005. Bloggers' expectations of privacy and accountability: An initial survey. J. Comput.-Mediated Commun., Vol. 10, No. 3. 10.1111/j.1083-6101.2005.tb00260.x

Walther, J.B., 1996. Computer-mediated communication: Impersonal, interpersonal and hyperpersonal interaction. Commun. Res., 23: 3-43.

Walther, J.B., 2007. Selective self-presentation in computer-mediated communication: Hyperpersonal dimensions of technology, language and cognition. Comput. Hum. Behav., 23: 2538-2557.

Westin, A.F., 1970. Privacy and Freedom. The Bodley Head Ltd., London, UK., ISBN-13: 978-0370013251, Pages: 508.

Woon, I.M.Y., G.W. Tan and R.T. Low, 2005. A protection motivation theory approach to home wireless security. Proceedings of the 26th International Conference on Information Systems, December 11-14, 2005, Las Vegas, NV., USA., pp: 367-380.

Yao, M.Z. and A.J. Flanagin, 2006. A self-awareness approach to computer-mediated communication. Comput. Hum. Behav., 22: 518-544.

Youn, S., 2005. Teenagers' perceptions of online privacy and coping behaviors: A risk-benefit appraisal approach. J. Broadcasting Electron. Media, 49: 86-110.

Youn, S., 2009. Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. J. Consum. Affairs, 43: 389-418.

Zhang, L. and W.C. McDowell, 2009. Am I really at risk? Determinants of online users' intentions to use strong passwords. J. Internet Commerce, 8: 180-197.

Zheleva, E. and L. Getoor, 2009. To join or not to join: The illusion of privacy in social networks with mixed public and private user profiles. Proceedings of the 18th International Conference on World Wide Web, April 20-24, 2009, Madrid, Spain, pp: 531-540.

Zlatolas, L.N., T. Welzer, M. Hericko and M. Holbl, 2015. Privacy antecedents for SNS self-disclosure: The case of Facebook. Comput. Hum. Behav., 45: 158-167.