Asian Journal of Information Technology 15 (16): 2992-2998, 2016
ISSN: 1682-3915
© Medwell Journals, 2016

# Factor Motivating Privacy Protection Behaviour Strategies and Information Privacy Concern in 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, Universiti Teknikal Malaysia, Melaka, Malaysia
[2]Center for Teaching and Learning, Universiti Teknikal Malaysia, Melaka, Malaysia

**Abstract:** In this study, we present our quantitative research in identifying the relationship of elements in hyperpersonal framework with information privacy concern and privacy protection behaviour. Hence, this study explains the roles of information privacy concerns in social networking sites by investigating the factors as well as ehavioural strategies that individual use in protecting their privacy. An empirical study engaged a total of 488 ndergraduates 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. Findings of this study show that information privacy concern has positive relationship towards privacy rotection behaviour. Perceived anonymity of others and perceived intrusiveness are found to be the factors of nformation privacy concern.

**Key words:** Social networking sites, privacy protetion behaviour, information privacy concern, hyperpersonal ramework

## INTRODUCTION

Social Networking Sites (SNSs) have become a henomenon which has attracted many researchers rom a variety of disciplines including technology, ommunications and sociology in the last few years Zlatolas *et al*., 2015). According to Statista (2016), pproximately two billion internet users use SNSs as f April 2016 and these figures are expected to grow. Due to the high increase of users in SNSs, concerns bout the vulnerability of users to privacy risks and hreats have been raised. A study on privacy has aised a considerably monumental amount of ttention amongst researchers due to the massive mount of personal information gathered, stored and hared when using SNSs. Disclosure of personal information among SNS users, whether consciously r not, has exposed them to dangers, threats and isks. Once a picture or post goes online, users are owerless to stop others from cutting, pasting and haring their content. The SNSs have also been provided ith privacy settings and privacy policies to control nd customize the information shared with other sers. Unfortunately, research suggests that it is not nough to protect one's sensitive data (Zheleva and Getoor, 2009). It has been statistically shown that though the concern towards privacy by users are ignificant, their attitude towards the risks of nformation disclosure is still very relaxed (Dhawan and Goel, 2014). Besides that, even when SNSs themeselves ave been equipped with systematic privacy features, t still cannot guarantee that one's privacy is fully rotected (Salleh *et al*., 2012).

Several theories and models have been used to explore the factors that contribute to information privacy concerns and privacy protection behaviours such as the Protection Motivation Theory (Marett *et al*. 2011; Mohamed and Ahmad, 2012; Youn, 2009), "Antecedents¬Privacy Concerns¬Outcome or "PCO" Macro Model (Jia *et al*., 2015; Xu *et al*., 2011) and Five-Factor Model of Personality also known as The Big Five (Korzaan and Boswell, 2008). With the former in mind, the use of the Hyperpersonal Framework in this study can enrich privacy-related studies by providing them with several fresh insights. This is thanks to the framework itself as it focuses on an approach that understands the relationship development in the mediated environment.

This study's aim is to enhance our understanding of information privacy concerns and privacy protection behaviours in SNSs by using the Hyperpersonal Framework. As proposed by Jiang *et al*. (2013) in their previous research on the study of privacy protection behaviour in synchronous online social interaction,

**Corresponding Author:** Nur Fadzilah Othman, Information Security and Networking Research Group (InForSnet), Center for Advanced Computing Technology, Universiti Teknikal Malaysia Melaka, Malaysia

adopting the Hyperpersonal Framework in asynchronous communication such as Facebook may have different findings because individuals may behave differently in asynchronous communication as compared to synchronous social interaction. Hence, this study proposes to refine the model from Jiang *et al.* (2013) and to test the refined model in Malaysia.

## Literature review

### Information privacy concern and privacy

**Protection behaviour:** According to a definition provided by Warren and Brandeis (1890), privacy is the right to determine the extent to which a person communicates his thought, sentiments and emotions and the right to be alone. The definition of information privacy as defined by Smith *et al.* (1996) is the individual's ability to personally control information about one's self. Additionally, the definition of 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 (Smith *et al.*, 1996).

Individuals will adopt various behavioural strategies to protect their privacy when they feel betrayed, have a sense of unfairness, inequality and emotional distress (Zwick and Dholakia, 2004). According to Goodwin, (1992), privacy protection refers to the management of personal information disclosure while deflecting unwanted intrusions. Rogers (1983) stated that individual motivation in protection occurs in coping behaviours to control danger and prevent threat and risks. Coping strategies when confronted in protecting privacy can be divided into two parts namely approach and avoidance (Feng and Xie, 2014; Jia *et al.*, 2015; Smit *et al.*, 2014). Coping by approach refers to confrontation strategies that encompass problem solving and seeking for social support whereas coping by avoidance lead users to ignore or refuse to use the websites in question. The strategies included in coping by approach are fabricating personal information and seeking social support by asking for information and advice or reading the privacy statement (Youn, 2009), while coping by avoidance approach consists of withholding and protecting the information (McDonald and Cranor, 2010). Privacy protection behaviour strategies in SNS environments can apply both approach and avoidance strategies in order to protect personal information. A few examples of an approach strategy is seeking advice from others about privacy issues in SNSs and reading the privacy statement in SNSs to obtain information on how SNS providers collect their information and how that information is used. Other approach strategies include fabricating or falsifying the information provided in SNSs. As for avoidance strategies, SNS users can withhold their information by refusing to provide or declining to join SNSs. They can also go to alternative sites that do not require disclosure of personal information. Each user may practice different protection strategies to protect themselves from risks and threats (Lwin and Ang, 2012). Many studies has been done and argue that information privacy concerns have a positive relationship towards privacy protection behaviours.

In the research by Jiang *et al.* (2013), it was found that the increase of information privacy concerns contribute to privacy protective bahaviours in synchronous online social interaction. Similarly, Mohamed and Ahmad (2012) stated that users will adopt privacy protection behaviours in SNSs if they are concerned with the threat and risk of losing privacy via the disclosure of personal information. Hence, It is important to behave in SNSs as behaviour towards privacy ultimately depends on appropriate end user behaviours (Rhee *et al.*, 2009).

**Hyperpersonal framework:** Hyperpersonal framework recommended by Walther (1996), suggests a strategy to understand how user experience relates to intimacy in a mediated communication medium. Hyperpersonal framework contains four elements of mediated communication, of which show how senders select, receivers magnify, channels promote and feedback facilitates the development of social relationships in the mediated environment (Jiang *et al.*, 2013). Hyperpersonal framework has been used in several studies to grasp relationship development in mediated environments. As an example, the sender's perspective helps clarify the effects of self-awareness on individual's social attractiveness in instant messaging (Yao and Flanagin, 2006) whereas the receiver's perspective explains impression management in teleconferencing (Gibbs *et al.*, 2011). For channel and sender characteristics, it is proven that in order to shape self-presentation behaviour in online dating websites, channel characteristic and feedback are essential elements (Gibbs *et al.*, 2011).

**Perceived anonymity of self:** Perceived anonymity of self was examined to reflect the sender's perspective. According to hyperpersonal framework, the sender's perspective is considered as a consequence of limited identity cues on individuals' impression management. The individuals will then focus on the information they have selectively sent to others (Jiang *et al.*, 2013). In doing so, users will focus on the personal information they have selectively sent to others. In SNSs, user can preserve their anonymity by completely or partially revealing their personal information. Individuals will feel responsible while going online if they feel there is someone else who knows their personal information (Ji and Lieber, 2010). Hence, if the users perceive themselves as anonymous or

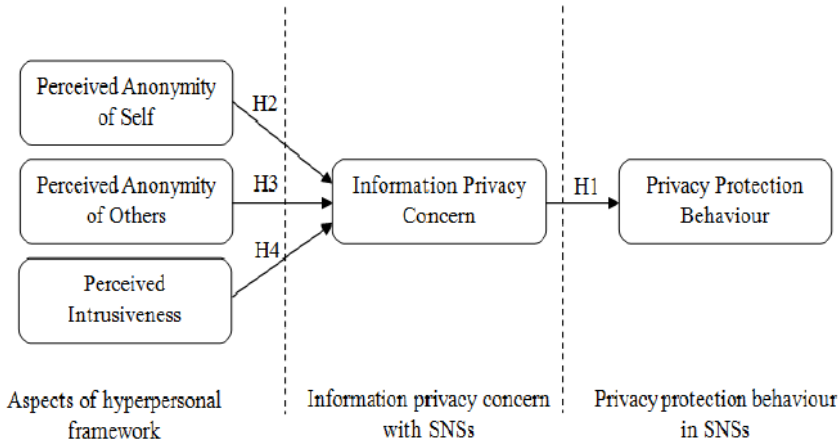


Fig. 1: Proposed research model

nidentifiable in SNSs, they feel secure against risks and threats from other users. Consequently, it will lead them to be less concerned about their information privacy.

**Perceived anonymity of others:** Perceived anonymity of others was examined to reflect the receiver's perspective.In order to establish the receiver's perspective, limited identity sign also plays an important role. Another person's identity can often be partial or fragmented and can at times, remain largely unidentifiable due to a lack of physical appearance in online social interactions (Jiang *et al*., 2013). Past studies identified that individuals feel anxious and paranoid about losing their privacy if they fail to know much about other parties within social interactions (Viegas, 2005) and individuals will become more acceptable and tolerant towards privacy loss when others provide adequate explanations (Colquitt, 2001). In this study, unidentifiable or anonymous persons in SNSs will increase an individual's information privacy concern within them.

**Perceived intrusiveness:** Perceived intrusiveness was examined to reflect the feedback perspective. In online interactions, feedback happens in the way personal information is exchanged and questions are asked or answers are provided in a to-and-fro manner (Jiang *et al*., 2013). To gain understanding from others, individuals will interpret other's feedback in social interaction (Walther, 1996). To control access to private information during exchanging information, individuals will usually maintain psychological boundaries (Petronio, 2002). Psychological boundaries can be split if individuals reveal personal information in response to requests from others. This, in turn might stimulate individuals' perceived intrusiveness due to the penetration of psychological boundaries (Vandebosch and Van Cleemput, 2009). An increase of perceived intrusiveness will increase information privacy concerns in SNSs. In this study, we hypothesize three aspects of hyperpersonal framework and information privacy concern. We also propose investigating the effects of information privacy concern towards privacy protection behaviours. Figure 1 shows the proposed research model for this study. The following hypotheses are as follows:

- $H_1$: Information privacy concern is positively related to privacy protection behaviour in social networking sites
- $H_2$: Perceived anonymity of self is negatively related to information privacy concern with social networking sites
- $H_3$: Perceived anonymity of others is positively related to information privacy concern with social networking sites
- $H_4$: Perceived intrusiveness is positively related to information privacy concern with social networking sites

Because existing theories and empirical evidence do not hint at a clear relationship between channel elements in hyperpersonal framework towards information privacy concern, we do not hypothesize on them.

## MATERIALS AND METHODS

In this study, a total of four hypotheses were tested. Thus, a quantitative approach was used to test them. Quantitative approach is the best method to use in order to test any existing theories as it involves the collection and statistical analysis of numerical data (Ary *et al*., 2010). The instrument used in this study was a questionnaire that consisted of 31 items. 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) and 7 items for privacy protection behaviour adapted from (Feng and Xie, 2014). All the items used a 5 point Likert scale where 5 represented trongly agree and 1 represented trongly disagree. responses.

**Sample selection and data collection:** For the sampling process, stratified random sampling approach was used. The accessible population consisted of undergraduates from the public Malaysian University. There were 9205 undergraduates in total. The ideal number for sample size suitable for analysis using SEM should approximately be between 300-800 samples (Sedek *et al*., 2012). Total 499 were returned from 550 distributed. For the purpose of this study, 485 were usable with a response rate of 88%. Table 1 shows the profile of the respondents.

**Data analysis:** The items for this instrument were validated by a group of experts from other public universities and Cyber Security Malaysia (CSM). We then piloted the instrument to 40 samples. Afterwards, the data was analyzed following procedures suggested by (Joreskorg, 1993). Based on procedures recommended by (Joreskorg, 1993), the full sample (N = 433) was divided into two data sets of calibration and validation.

Table 1: Profile of respondents

| Variable | Type | Frequency | Percent |
|---|---|---|---|
| Gender | Male | 254 | 52 |
| | Female | 231 | 48 |
| Age | 15-20 | - | - |
| | 21-25 | 449 | 93 |
| | 26-30 | 36 | 7 |

About 150 respondents were used as the calibration sample while the remaining 299 respondents were treated as the validation sample. The calibration sample (n-150) was examined using Exploratory Factor Analysis (EFA). The purpose of conducting EFA was to reduce the data set to a more manageable size whilst retaining as much of the original information as possible (Jabar, 2011). Consequently, the validation sample (n = 283) and the final version of questionnaires consisted of 23 items from 31 items. The AMOS program was used to analyze the data and to confirm selected item for each construct hence validating the framework.

## RESULTS AND DISCUSSION

According to Byrne (2013), Structural Equation Modeling (SEM) was applied to detect relationships among the constructs. SEM is more applicable for accessing constructs and relations between constructs as compared to the first generation methods such as multiple regressions. Besides, according to Cohen *et al*. (2013), the use of multiple regressions are not possible or practical because it has limited ability in identifying results for linear relationships and near intervals with limited range as well as being unable to evaluate the relationship between constructs or variables simultaneously. During SEM analysis, all fitness indexes must achieve the required level. Table 2 shows the set of criteria for fit indices and their recommended value. As shown in Table 3 is the result of the fitness indexes for research model. All required level was acheived.

The root mean square error of approximation (RMSEA) which measures the discrepancy per degree of freedom was 0.058, the Goodness-of-Fit Index (GFI) was 0.906, Comparative Fit Index (CFI) was 0.886 and discrepancy Chi-Square ($\chi^2$/df) was 2.551. Figure 2

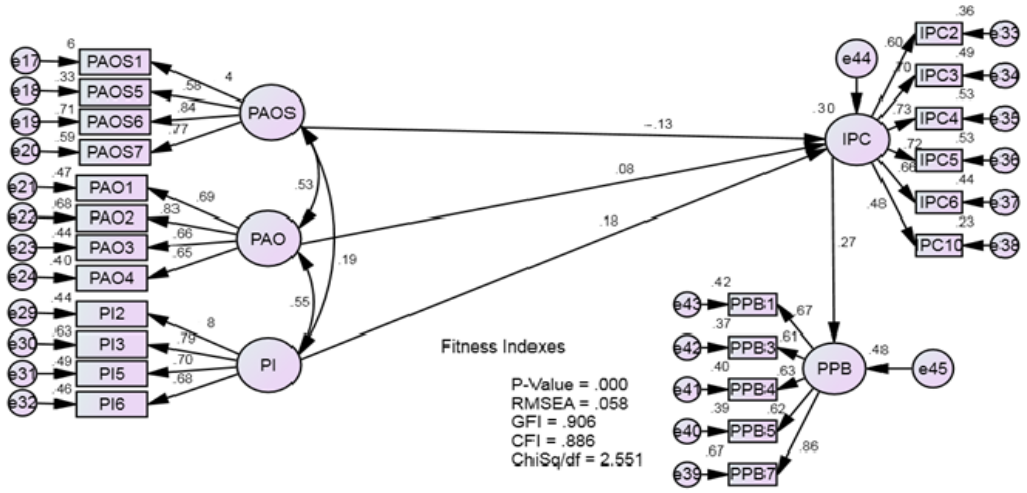


Fig. 2: Structural model

Table 2: Categories of model fit and their level of acceptance

| Name of catagories | Name of index | Level of acceptance | Sources |
|---|---|---|---|
| Absolute fit | RMSEA | ≤0.08 | Awang, (2012), Baumgartn |
| Incremental | GFI | ≥0.8 | and Homburg (1996), Doll *et al.* (1994) |
| | CFI | ≥0.8 | Baumgartn er and Homburg, (1996), Doll *et al.* (1994) |
| Parsimonio | $\chi^2$/df | 3.0 | Awang (2012) |

Table 3: The fitness Indexes for research model

| Name of catagories | Name of index | Level of acceptance | Sources |
|---|---|---|---|
| Absolute fit | RMSEA | 0.058 | The required level is achieved |
| Incremental | GFI | 0.906 | The fit required level is achieved |
| | CFI | 0.886 | The required level is achieved |
| Parsimonious | $\chi^2$/df | 2.551 | The fit required level is achieved |

Table 4: The regression path coefficients, significance value 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: Information privacy concern is positively related to privacy protection behaviour in social networking sites | 0.27 | 0.001 | Supported |
| PAOS--> | IPC | H2: Perceived anonymity of self is negatively related to information privacy concern with social networking sites | -0.13 | 0.017 | Supported |
| PAO--> | IPC | H3: Perceived anonymity of others is positively related to information privacy concern with social networking sites | 0.08 | 0.023 | Supported |
| PI--> | IPC | H4: Perceived intrusiveness is positively related to information privacy concern with social networking sites | 0.18 | 0.010 | Supported |

could be seen that this proposed model was able to explain 23% of the variance in information privacy concern and 38% of the variance in privacy protection behaviour among undergraduates. As compared to the one introduced by Jiang *et al.* (2013), their model was only capable of explaining a total of 20% of variance in information privacy concern and 31% variance for privacy protection behaviour. A summary of regression path coefficient value and hypothesis statement for every path and its conclusion is shown in Table 4.

## CONCLUSION

This study has enhanced the understanding in information privacy concern, its factors and privacy protection behaviour. It is shown via this study's results that if users are indeed concerned about their privacy in SNSs, they would use privacy protection strategies. Based on hyperpersonal framework, three factors contributed to information privacy concern. After the empirical analysis, all the factors appeared as significant factors to information privacy concern and all the hypotheses were accepted. Although, the study was conducted in a different context, namely asynchronous social networks, the findings of this study was found to be in line with previous studies conducted by Jiang *et al.* (2013) as performed within synchronous online social interactions. Our findings confirm that constructs derived from hyperpersonal framework are important factors of information privacy concern and privacy protection behaviour. Individuals who are concerned about their privacy in SNSs have been found to adopt privacy protection behavior strategies. This is supported by prior research as conducted by Jiang et al., (2013), Mohamed and Ahmad (2012) and Youn (2009). Hence, it is essential to increase user's concerns towards privacy in order to encourage them to adopt privacy protection behaviours.

Perceived anonymity of self was found to be one of the factors that contribute to information privacy concern. This factor contributes a negative relationship towards information privacy concern. SNS users who perceive themselves as unidentifiable or anonymous will become less concerned about their information privacy because they feel protected against being scrutinized or ridiculed by other users. This finding supports the second hypothesis of this study which proposed that perceived anonymity of self is negatively related to information privacy concern within social networking sites. Perceived anonymity of others and perceived intrusiveness have also been found as factors that contribute to information privacy concern. Supporting the third and fourth hypotheses, these factors contribute a positive relationship towards information privacy concern. Users feel threatened and will be afraid of losing their privacy if they fail to know much about other individuals of whom they interact with in SNSs. Past studies that support this research done by Jiang *et al.* (2013) has found that perceived anonymity of others will increase privacy concern in online chat.

Finally, individuals that feel disturbed in SNSs will increase their concern towards privacy as well as adopt privacy strategies in order to secure themselves. With this, it is proven that perceived intrusiveness would

increase information privacy concern in SNSs. In conclusion, this research is very important in providing a guideline for users to protect their privacy in SNSs. This finding may also provide beneficial information to site providers and trigger a redesign of privacy protection strategies. On behalf of educators, the instrument may be used to evoke users' information privacy concern and use of privacy protection strategies in SNSs. Appropriate programs with aims to create awareness towards privacy issues in SNSs can be identified by institutions and include risk and threats of SNSs, consequences from losing information, privacy awareness and effective privacy protection behavior in SNSs.

## 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.

Awang, Z., 2012. A Handbook on SEM: Structural Equation Modeling. 4th Edn., Centre For Graduate Studies, Kuala Lumpur, Malaysia.

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.

Byrne, B.M., 2013. Structural Equation Modelling with Lisrel, Prelis and Simplis: Basic Concepts, Applications and Programming. 3rd Edn., Lawrence Erlbaum Associates Inc, Mahwah, New Jersey, ISBN:0-8058-2924-5,.

Cohen, J., P. Cohen, S.G. West and L.S. Aiken, 2003. Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences. 3rd Edn., Routledge, Mahwah, NJ., USA., ISBN-13: 9780805822236, Pages: 703.

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

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.

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.

Goodwin, C., 1992. A conceptualization of motives to seek privacy for nondeviant consumption. J. Consum. Psychol., 1: 261-284.

Jabar, J., 2011. An empirical study of strategic technology alliances and the performance of Malaysian manufactures. Msc Thesis, University of South Australia, Adelaide, South Australia.

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

Jia, H., P.J. Wisniewski, H. Xu, M.B. Rosson and J.M. Carroll, 2015. Risk-taking as a learning process for shaping teen's online information privacy behaviors. Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work and Social Computing, February 14-15, 2015, ACM, Vancouver, British, ISBN:978-1-4503-2922-4, pp: 583-599.

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.

Joreskog, K.G., 1993. Testing Structural Equation Models. In: Testing Structural Equation Models, Bollen, K.A. and J.S. Long (Eds.). Chapter 12, Sage Publication, Newbury Park, CA., USA., ISBN-13: 978-0803945074, pp: 294-316.

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.

Lwin, M.O., B. Li and R.P. Ang, 2011. Stop bugging me: An examination of adolescents protection behavior against online harassment. J. Adolescence, 35: 31-41.

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.

McDonald, A.M. and L.F. Cranor, 2010. Americans attitudes about internet behavioral advertising practices. Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society, October 4-8, 2008, ACM, Chicago, Illinois, ISBN:978-1-4503-0096-4, pp: 63-72.

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.

Rhee, H.S., C. Kim and Y.U. Ryu, 2009. Self-efficacy in information security: Its influence on end users information security practice behavior. Comput. Secur., 28: 816-826.

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

Sedek, M., R. Mahmud, H.A. Jalil and S.M. Daud, 2012. Types and levels of ubiquitous technology use among ICT undergraduates. Procedia-Social Behav. Sci., 64: 255-264.

Smit, E.G., V.G. Noort and H.A. Voorveld, 2014. Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. Comput. Hum. Behav., 32: 15-22.

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

Statista, 2016. Leading global social networks 2016. Statista Database company, http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

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.

Warren, S.D. and L.D. Brandeis, 1890. The right to privacy. Harvard Law Rev., 4: 193-220.

Xu, H., T. Dinev, J. Smith and P. Hart, 2011. Information privacy concerns: Linking individual perceptions with institutional privacy assurances. J. Assoc. Inf. Syst., 12: 798-824.

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

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

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.

Zwick, D. and N. Dholakia, 2014. Whose identity is it anyway? Consumer representation in the age of database marketing. J. Macromarketing, 24: 31-43.