INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 15, Issue 3, (2025) E-ISSN: 2222-6990

Key Drivers of Privacy Protection Behavior in Social Networking Sites: A Motivational Perspective

Muliati Sedek[1], Teh Zanariah Mohd Raus[2], Nur fadzilah Othman[3]

[1,2]Center for Language Learning, Universiti Teknikal Malaysia Melaka, 76100 Durian Tunggal, Melaka, [3]Faculty of Information Technology and Communication, Universiti Teknikal Melaka, 76100 Durian Tunggal, Melaka

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v15-i3/25164 DOI:10.6007/IJARBSS/v15-i3/25164

Published Date: 27 March 2025

Abstract

The increasing prevalence of social networking sites (SNSs) has raised concerns about users' privacy protection behavior. Despite the presence of privacy settings and policies, users often engage in behaviors that expose them to potential privacy breaches. This study investigates the key determinants influencing privacy protection behavior on SNSs, guided by the Protection Motivation Theory (PMT). Specifically, the study examines the role of perceived severity, perceived vulnerability, response efficacy, self-efficacy, and information privacy concerns in shaping users' privacy protection strategies. A quantitative research approach was employed, utilizing a structured questionnaire distributed to undergraduate students in Malaysia. A total of 485 valid responses were analyzed using Structural Equation Modeling (SEM) to assess the relationships between the variables. The findings reveal that perceived severity, perceived vulnerability, self-efficacy, and response efficacy significantly influence information privacy concerns, which, in turn, drive users to adopt privacy protection behaviors. However, reward was found to have no significant impact on information privacy concern. These results underscore the importance of enhancing users' awareness and confidence in managing their online privacy. The study contributes to both theory and practice by offering insights into how SNS users perceive and respond to privacy threats, thereby informing the development of more effective privacy education and intervention strategies.

Keywords: Privacy Protection Behavior, Social Networking Sites, Information Privacy Concern, Protection Motivation Theory, Structural Equation Modeling

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 utilization 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 behavior strategies that have been employed by users while utilizing SNSs. By understanding the determinants of privacy protection, it 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 behavior strategies.

Privacy Protection Behavior Strategies

Privacy has been defined in various ways across different disciplines. In law, it is seen as the "right to be alone" (Warren & Brandeis, 1890), while in philosophy, it is understood as a "state of limited access" (Schoeman, 1984). From a social science perspective, privacy is about having "control over information about oneself" (Kokolakis, 2017).

When it comes to privacy protection behavior, it refers to specific actions people take to safeguard their personal information online. According to Rogers (1983), individuals are driven to adopt protective behaviors as a way to manage risks, threats, and potential dangers. These strategies are generally categorized into two approaches: approach and avoidance (Chen, Beaudoin & Hong, 2017). Approach strategies involve tactics like fabricating personal information (e.g., using fake names or false details on social networking sites) and seeking social support (such as reading privacy policies or asking for advice on how to protect their data). On the other hand, avoidance strategies include withholding personal information, meaning users may choose not to share sensitive details online or even actively challenge platforms that request excessive personal data.

At the heart of privacy protection is information privacy concern, which reflects how much individuals worry about how organizations collect and use their personal data (Martin, Borah & Palmatier, 2017). Studies have shown that people with higher privacy concerns tend to engage more in privacy protection behaviors (Sedek & Mohd, 2025). Within Protection Motivation Theory (PMT), privacy concern plays a key role as a mediator, helping to explain how different factors influence a person's decision to adopt privacy-protecting behaviors. In essence, the greater the concern, the more likely individuals are to take action to safeguard their personal information online.

Theoretical Framework and Hypotheses

Protection Motivation Theory

Protection Motivation Theory (PMT), introduced by Rogers (1975), suggests that an individual's motivation to safeguard themselves against threats arises from three key factors: (1) perceived severity, (2) perceived vulnerability, and (3) response efficacy. The model was later refined to address failures in protective behavior by incorporating additional factors: (4) self-efficacy, (5) response cost, and (6) rewards linked to risky behavior (Rogers, 1975; 1983).

While PMT has been predominantly applied in the health sector (Grindley, Zizzi, & Nasypany, 2008) and utilized in over 20 different health-related fields to study behavioral intentions, it has also been widely adopted in Information Systems (IS) research. In this domain, PMT has been used to explore online protection behaviors, employees' awareness of organizational security policies, and individuals' use of security software (Johnston & Warkentin, 2010).

Perceived Severity

Perceived severity refers to an individual’s assessment of the seriousness of a potential threat and its consequences (Palladini et al., 2017). It evaluates how significantly a person believes a threat can disrupt their life, influencing their decision to take preventive measures. Individuals are more likely to adopt recommended actions when they perceive severe consequences. Adhikari and Panda (2017) found that perceived severity strengthens motivation to engage in risk-reducing behaviors. In the context of this study, users who experience a loss of information privacy on social networking sites (SNSs) will develop a heightened sense of perceived severity, leading to greater concern over their privacy. This, in turn, serves as an indirect motivator for adopting privacy protection strategies on SNSs.

Perceived Vulnerability

Perceived vulnerability describes an individual’s perception of their susceptibility to negative consequences resulting from risky behavior (Kim & Kim, 2016). Research suggests that heightened perceived vulnerability increases students’ intention to avoid malware risks. Similarly, Schoeman (1984) emphasized that perceived vulnerability is a significant factor contributing to rising concerns over information privacy. However, some findings suggest otherwise; for instance, Kokolakis (2017) found that perceived vulnerability does not significantly influence employees’ willingness to comply with information security policies. In this study, it is proposed that individuals who acknowledge the risks and threats of losing personal data on SNSs will develop stronger privacy concerns, which, in turn, motivate them to adopt privacy protection strategies.

Self-Efficacy

Self-efficacy is defined as an individual’s confidence in their ability to effectively implement protective measures while using SNSs (Compeau, Higgins, & Huff, 1999). Research highlights self-efficacy as a key factor influencing users’ engagement in risky online behavior. Lee et al. (2008) suggest that self-efficacy plays a pivotal role in encouraging protective behavior. Thus, this study posits that individuals who feel confident in their ability to manage privacy settings and security measures on SNSs are more likely to be concerned about their information privacy and take proactive steps to protect themselves.

Response Efficacy
Response efficacy refers to the belief that taking preventive actions will effectively mitigate a threat (Grindley et al., 2008). Research has identified response efficacy as a strong predictor of whether individuals decide to implement security measures, such as enabling security features on networks, using anti-spyware software, backing up personal data, and employing malware protection tools (Martin et al., 2017). This study suggests that individuals who have greater confidence in the effectiveness of privacy protection strategies will be more proactive in safeguarding their personal data, ultimately reducing their risk of privacy breaches.

Rewards
Rewards refer to the anticipated benefits individuals expect to gain from engaging in a specific behavior (Lee et al., 2008). Previous studies indicate that individuals who derive enjoyment and satisfaction from sharing personal information are less likely to take protective actions (Marett, Harris, & McNab, 2011).

Moreover, some users believe that sharing personal information fosters a sense of closeness with friends and family, leading to greater social satisfaction. As a result, individuals who prioritize these social rewards may be less motivated to adopt privacy protection behaviors despite potential risks.

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 (Sedek & Mohd, 2025).

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.

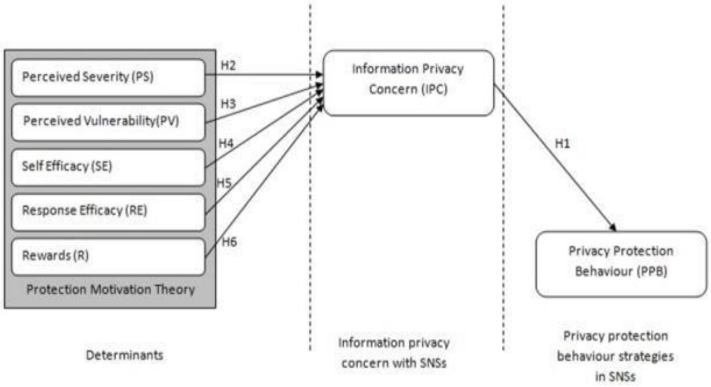

Perceived Severity (PS)
Perceived Vulnerability(PV)
Self Efficacy (SE)
Response Efficacy (RE)
Rewards (R)
Protection Motivation Theory
H2
H3
H4
H5
H6
Information Privacy Concern (IPC)
H1
Privacy Protection Behaviour (PPB)
Determinants
Information privacy concern with SNSs
Privacy protection behaviour strategies in SNSs

Figure 1: Proposed Research Model

Research Methodology

This study tested a total of six hypotheses using a quantitative approach, which was deemed the most suitable method for examining existing theories. A quantitative approach allows for the systematic collection and statistical analysis of numerical data (Ary, Jacobs, Razavieh, & Sorensen, 2010). The research instrument utilized was a questionnaire that comprised of 44 items, all measured using a five-point Likert scale, where 5 indicated "strongly agree" and 1 indicated "strongly disagree."

Sample Selection and Data Collection

This study employed stratified random sampling to select participants. Based on data provided by the universities' administration, as of February 26, 2015, the total number of active undergraduate students was approximately 9,205. Following the recommendation by Sedek, Mahmud, and Jalil (2012), the ideal sample size for Structural Equation Modeling (SEM) analysis should range between 300 to 800 respondents. A total of 550 questionnaires were distributed, with 499 responses received. After data screening, 485 responses were deemed valid for analysis, resulting in an 88% response rate. Table 1 presents the demographic profile of the respondents.

Table 1
Demographic profile

Variable	**Type**	**Frequency**	**Percent**
Gender	Male	254	52
	Female	231	4
Age	15-20	-	-
	21-25	449	93
	26-30	36	7
	31-35	-	-

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.

Table 2
Overall model fit

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 represents the Structural Equation Modeling (SEM) analysis confirms that perceived severity, perceived vulnerability, self-efficacy, and response efficacy significantly influence information privacy concern (IPC), which in turn drives privacy protection behavior (PPB). Individuals who perceive greater risks, believe in their ability to manage privacy, and trust the effectiveness of protective measures are more likely to be concerned about their privacy and take protective actions. However, reward does not significantly impact IPC, suggesting that incentives do not strongly influence privacy concerns. The model fit indices (P-value = 0.000, RMSEA = 0.055, GFI = 0.851, CFI = 0.882, and Chi-square/df = 2.964) indicate a well-fitted model, reinforcing the reliability of these relationships in explaining privacy-related behaviors.

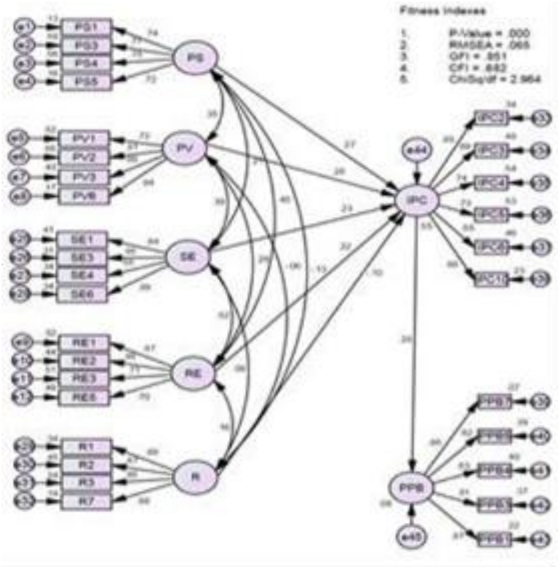
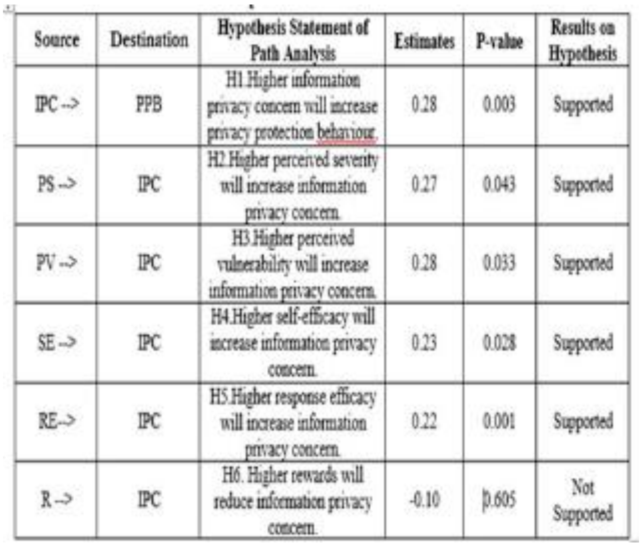


Figure 2: The Structural Model

Table 3
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

Table 3 is the analysis of the Structural Equation Modeling (SEM) results. The results confirm that five out of six hypotheses were supported, demonstrating significant relationships between various determinants and information privacy concerns (IPC). The findings indicate that higher levels of IPC lead to an increase in privacy protection behavior (PPB) (β = 0.28, p = 0.003). Additionally, perceived severity (PS) (β = 0.27, p = 0.043), perceived vulnerability (PV) (β = 0.28, p = 0.033), self-efficacy (SE) (β = 0.26, p = 0.028), and response efficacy (RE) (β = 0.22, p = 0.001) were all found to significantly enhance concerns about information privacy. However, the hypothesis suggesting that higher rewards (R) would reduce information privacy concerns was not supported (β = -0.10, p = 0.605), implying that incentives or rewards do not significantly influence individuals' concerns about their privacy. These results suggest that individuals who perceive a greater risk, believe in their ability to manage their privacy, and trust the effectiveness of protective strategies are more likely to be concerned about their information privacy, subsequently adopting protective behaviors.

Conclusion

The Structural Equation Modeling (SEM) analysis indicates a significant relationship between perceived severity, perceived vulnerability, response efficacy, and self-efficacy with concerns about information privacy. Additionally, a strong link was identified between information privacy concerns and the implementation of privacy protection strategies. Consistent with previous studies, individuals who are more concerned about their information privacy on social networking sites (SNSs) tend to adopt and utilize privacy protection behaviors (Kim & Kim, 2016). Several key factors contribute to shaping this concern and awareness. One such factor is perceived severity, where users who believe that a loss of information privacy will have serious consequences exhibit greater concern, whereas those who perceive minimal impact are less worried.

Another key determinant significantly linked to information privacy concerns is perceived vulnerability. The findings indicate that individuals who have experienced or are at risk of losing their information privacy express higher levels of concern. In contrast, those who have not faced such risks demonstrate lower concern.

Self-efficacy also plays a crucial role in shaping information privacy concerns. Individuals who believe in their capability to implement protective strategies on SNSs are more likely to be concerned about their privacy. Similarly, response efficacy, which refers to users' confidence in the effectiveness of privacy protection measures, contributes to their level of concern regarding information privacy. However, one factor, reward, was found to have no significant association with information privacy concerns, contradicting the initial hypothesis of the study.

The significance of this research lies in its multifaceted contributions to both theoretical advancement and practical applications. Theoretically, this study extends the Protection Motivation Theory (PMT) by validating its constructs in the context of privacy behavior on social networking sites (SNSs), particularly among Malaysian youth. The incorporation of information privacy concern as a mediating variable offers a nuanced understanding of how threat and coping appraisals interact to shape behavioral outcomes in digital environments. This contributes to the growing body of literature on privacy behavior by providing empirical evidence from a non-Western context, thereby enhancing the generalizability of PMT in online privacy research.

Practically, the findings have far-reaching implications for educators, policymakers, system designers, and digital literacy advocates. For instance, interventions and awareness programs aimed at improving privacy behavior among SNS users can be designed to specifically enhance self-efficacy and response efficacy, which were shown to be significant predictors. This could include user training modules, privacy management tutorials, or even gamified platforms that simulate privacy threat scenarios to boost users' confidence and skills. System designers and SNS platforms can also utilize these insights to improve interface designs—making privacy settings more visible, intuitive, and customizable to encourage proactive user behavior. Furthermore, the study provides valuable insights for policymakers in developing national digital safety strategies and educational curricula that emphasize online privacy, especially in a rapidly digitizing society like Malaysia.

In summary, by highlighting the psychological mechanisms that influence online privacy protection, this research not only bridges the gap between theory and practice but also paves the way for more effective, data-informed privacy interventions and technologies that empower users to better control their digital identities.

References

Adhikari, K., & Panda, R. K. (2017). Users' information privacy concerns and privacy protection behaviors in social networks: Evidence from India.

Ary, D., Jacobs, L. C., Sorensen, C., & Razavieh, A. (2010). *Introduction to research in education* (8th ed.). Wadsworth Cengage Learning.

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. https://doi.org/10.1177/1354856507084416

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. https://doi.org/10.1016/j.chb.2017.01.014

Compeau, D., Higgins, C. A., & Huff, S. (1999). Social cognitive theory and individual reactions to computing technology: A longitudinal study. *MIS Quarterly, 23*(2), 145–158. https://doi.org/10.2307/249749

Grindley, E. J., Zizzi, S. J., & Nasypany, A. M. (2008). Use of protection motivation theory, affect, and barriers to understand and predict adherence to outpatient rehabilitation. *Physical Therapy: Journal of the American Physical Therapy Association, 88*(12), 1529–1540. https://doi.org/10.2522/ptj.20070318

Johnston, B. A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *Journal of the Ministry of Education Official Website, 34*(3), 549–566.

Kim, A. Y., & Kim, T. S. (2016). Factors influencing the intention to adopt identity theft protection services: Severity vs. vulnerability. In *Proceedings of the Pacific Asia Conference on Information Systems (PACIS)* (p. 68).

Kokolakis, S. (2017). Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Malaysian Communications and Multimedia Commission (MCMC). (2014). *Communications & multimedia pocket book of statistics*.

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.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing, 81*(1), 36–58. https://doi.org/10.1509/jm.15.0497

Nemec Zlatolas, L., Welzer, T., Heričko, M., & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior, 45*, 158–167. https://doi.org/10.1016/j.chb.2014.12.012

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. https://doi.org/10.3389/fpsyg.2017.01524

Salleh, N., Hussein, R., Mohamed, N., Abdul, N. S., Ahlan, A. R., & 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*, 1–12.

Schoeman, F. (Ed.). (1984). *Philosophical dimensions of privacy: An anthology*. Cambridge University Press.

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. https://doi.org/10.1016/j.sbspro.2012.11.030

Sedek, M., & Mohd, C. K. N. C. K. (2025). Exploring Educators' Perception of and Readiness for Hybrid Flexible Learning in Technical and Vocational Education and Training (TVET) in Higher Education. *Scientific Journal of King Faisal University: Humanities and Management Sciences*.

Vithessonthi, C. (2010). Knowledge sharing, social networks, and organizational transformation. *The Business Review, Cambridge, 15*(2), 99–109.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220.