Determinants of Privacy Protection Behavior in Social Networking Sites

Siti Norlyana Suhaimi[1], Nur Fadzilah Othman[2]*, Raihana Syahirah[3]
Syarulnaziah Anawar[4], Zakiah Ayop[5], Cik Feresa Mohd Foozy[6]
Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka, Malaysia[1]
Center for Advanced Computing Technology, Fakulti Teknologi Maklumat dan Komunikasi
Universiti Teknikal Malaysia Melaka, Malaysia[2, 3, 4, 5]
Faculty of Computer Science and Information Technology, Universiti Tun Hussien Onn, Malaysia[6]

***Abstract*—Social Networking Sites (SNSs) are an attractive online platform for social interaction and communication. Since SNSs are easily accessed by a large number of people, a large quantity of data is also stored in the SNSs. Consequently, concern regarding the exposure to privacy risk will emerge. In this case, users need privacy protection behavior to protect their privacy in SNSs. This paper aims to determine the motivational determinants of privacy protection behavior among high school students in protecting their data or personal information when using SNSs. To identify the determinants of privacy protection behavior, a questionnaire survey was administered on 200 high school students. This study proposed a conceptual model that offers an understanding of motivational determinants of privacy protection behavior in social networking sites. Results indicate that perceived anonymity is the most significant determinant in motivating privacy behavior followed by perceived intrusiveness, perceived severity, self-efficacy, perceived vulnerability, and response efficacy. The results of this study will shed some light on understanding the levels of privacy protection behavior in SNSs, and identify suitable interventions in motivating privacy protection behavior among high school students. Finally, with the combined theory of Protection Motivation Theory (PMT) and Hyperpersonal Communication Theory (HCT), this model provides the basis to direct future studies in the related field.**

Keywords*—Privacy; social networking sites; privacy; protection motivation theory; hyperpersonal communication theory

I. Introduction

As technology evolves, the user of the technology also increases. Nowadays, people use technology and SNSs as a platform to build social networks by communicating with friends, knowledge sharing, updating others on their activities and whereabouts, sharing photos, videos, archiving events, getting updates on activities by friends, sending messages privately, and posting public testimonials. SNSs offer an attractive way for social interaction and communication, thus encourages public users to use them. The rapid development of current technology in addition to the various attractive SNSs applications is driving the increase in the number of users. SNSs have become a major platform in carrying out various activities.

SNSs technology is capable of storing and sorting huge quantities of data and is easily accessed by a large number of people [1], which may unnecessarily expose them to various threats. The wide variety of features in the SNSs will influence people to expose their data privacy by sharing their personal information when utilizing SNSs. Consequently, concerns regarding the exposure to privacy risks emerge. Acts and behaviors show by users when utilizing SNSs will affect their lives either positively or negatively. This is because action towards privacy essentially relies on the behavior of the user itself. If users were not careful while utilizing the SNSs, it will have a detrimental effect on their lives instead of adding beneficial effects. While many users state that they stay informed about the risks in SNSs, this does not necessarily mean that they have the skills or motivation to behave securely [2].

Therefore, this study aims to identify the determinants of privacy protection behavior when utilizing SNSs among high school students in Malaysia. By knowing the determinants of privacy protection behavior, it will be able to provide knowledge that can protect users and empower them to assert their self-control with confidence through the implementation of strategies for privacy protection.

II. Literature Review

A. Privacy Protection Definition

Privacy is the right or power to monitor the distribution or release of details about a user or their actions. Privacy can be hard to protect these days due to the user's lack of knowledge of privacy protection. Privacy security protects the user details to avoid slipping into the hands of hackers, political agencies, and other organizations [3]. The concept of privacy protection varies from person to person [4] because each individual has specific privacy standards, and the degree of protection they need to believe. There are scientific and analytical cases where privacy protection can both enhance and subtract from the wellbeing of people and communities. Privacy protection shall keep user personal data from individuals who may attempt to misuse it. Minimizing user digital footprint makes it easier for people to take advantage of user data and users. If an attacker has good or bad intentions, the user's digital footprint will say a lot about them. An attacker will predict what users are doing every day, what users are doing in their leisure time, where users are working, moreover user's social activities, and all of their personalities [5]. Thus, protecting privacy involves data protection against unwanted access [6].

*Corresponding Author

B. Privacy Issues of Social Networking Sites (SNSs)

Once an individual had involvement in SNSs, they will contribute to various privacy issues [7]. There are endless examples of data being collected without the consent of a person, identities being generated based on SNSs usage, accounts being hacked, etc. According to [8], the growing number of cases of fraud, identity theft, cyberbullying, cyberstalking, and others were seen as a crucial enabler for improving users' trust in using SNSs.

Instead of the personal information that usually got stolen from the SNSs user, the user always forgot that they may reveal too much of their private information by themselves by sharing photos or videos on the SNSs. In the context of Malaysia, there is nothing that the legal system in Malaysia can do to secure users when those kinds of data got stolen [9]. A survey by the MCA's Civil Protection and Grievances Office shows that the loss of RM4.5 million had been reported due to identity fraud from 2014 to 2017 [10].

Malaysian Communication and Multimedia Commission (MCMC) has advised SNSs users not to treat SNSs as a personal diary [11]. Through the monitoring of MCMC, it is found that users often share personal information, photos, and locations that can attract persons with malicious intent. According to statistics by [12] in Incident Statistic Report 2019, there were a total of 10,772 incidents reported in 2019, and fraud cases are the highest. SNSs are one of the mediums used by scammers to find the victims of their fraud activities. Personal information displayed on SNSs to some extent becomes a source of initial information in locating potential victims. Corresponds with the study by [13], it argues that the SNSs should be a place where the user could have fun to share about their life with everyone, but still secure and confidential. Nowadays it seems to be a minefield for an attacker to hack, steal private information, data monitoring, and networking exploitation. Thus, SNSs today is being more anti-social and intrusive of privacy.

III. Theoretical Framework

This section provides the theoretical framework explaining the concept and the determinants of privacy protection behavior in SNSs. The proposed theoretical framework is based on the Protection Motivation Theory and Hyperpersonal Communication Theory.

A. Protection Motivation Theory

The Protection Motivation Theory (PMT) offers analytical insight to explain the attraction of apprehension in individuals and the difference in actions against certain situations or environments [14]. The development of PMT was to understand the reason for users who are concerned about protecting themselves from potential risks and helping to enhance the knowledge of determinants that make a user conduct relevant, prescribed behavior and ensuring the safety of privacy. A rising number of studies have stated the PMT's importance to understand responses of the user to privacy threats on SNSs [15]. Prior research has already shown the significance of the perceptions and behavior regarding privacy. A user who is more engaged in privacy protection behavior is a user who cares and cautious about information privacy and attaches high priority to their privacy protection [14]. Furthermore, the more the user face the privacy issues, the higher the protective behavior goes [16].

PMT consists of five factors: Perceived Vulnerability (PV), Perceived Severity (PS), Self-Efficacy (SE), Response Efficacy (RE), and Reward (R). The PMT states that the motivation of users to protect themselves against particular threats is based on two matters which are a threat appraisal and a coping appraisal. For threat appraisal, it measures the perceived severity of the threats and the perceived vulnerability to those threats. For coping appraisal, it measures self-efficacy and response efficiency. Both of the appraisals affect the behavior of the user to protect their privacy from a threat. Those appraisals have connections when both of them are perceived as high, where users will have the encouragement and motivation to have protection behavior to protect them from the threats and change their behavior.

1) Perceived Severity (PS): Perceived severity is best described as the perceived seriousness of threatening outcomes. User changes their behavior according to the perceived severity of the consequence and thus reduce the risk of threats. Perceived severity generally refers to the user's assumption that a threatening occurrence arises from a conclusion of severity significance [17]. Additionally, [18] stated that perceived severity can enhance a user's willingness to participate in the behavior of lessening the threat. Simply put, a greater level of perceived severity intensity will force internet users to take protective measures in SNSs [19]. Although a significant effect of perceived severity on intention and behavior has been found by several researchers, there is also evidence that shows that the severity is not significantly related to intention [20].

2) Perceived Vulnerability (PV): Perceived vulnerability is the decision of a user as to the probability of a threat. Alternatively, perceived vulnerability describes when the user did experiences the negative impact in SNSs, it will make the user motivated and implement protection behavior [21]. Several studies support the notion of perceived vulnerability that has a beneficial impact on defense actions by users. Perceived vulnerability has been found to increase students' intent to perform threat avoidance behaviors [22]. Furthermore, if people find themselves more vulnerable to an adverse danger, they take defensive measures to mitigate the danger. Additionally, when individuals perceive themselves to be vulnerable to privacy risks, they seem to be more worried about their personal information [23], which causes an emotional reaction and anxiety, which in effect raises the desire for defense [24].

3) Self-efficacy (SE): Self-efficacy can be defined as the degree to which users believe they should implement the recommended behavior. Users should have the courage to resolve difficulties that prohibit them from taking a specific action. Studies found that in the sense of privacy environments, users must have specific technological skills. This is linked to one's desire to change one's unsafe or inefficient behavior. In his study, [25] argues that one can also strengthen one's

actions toward more effective data protection initiatives with self-efficacy. When exchanging information, the user with better trust in their abilities to handle their privacy details may have fewer privacy issues [26]. Furthermore, [27] described self-efficacy as a core determinant of privacy protection or threat avoidance actions and a major factor in enhancing the effectiveness of the protection. This research attempts to identify the function of users' self-efficacy in the implementation of privacy protection behavior. As [28] stated that actual behavior is the main factor that affects self-efficacy. Hence, the role of the user's behavior as a basis of perceptions regarding self-efficacy has been largely established and confirmed.

4) Response Efficacy (RE): Response efficacy measures how effective the adoption of response in mitigating the threat. A study found that response efficacy is a major predictive activity that decides whether to introduce security measures on their networks or not, increases efforts to use anti-spyware as a protective tool, and predict backup of data on private computers [29]. Besides, [27] said that response efficacy is expected to take on a major role in reducing SNSa threats because the privacy of information is considered a question of ambiguity. Users that perceive improved privacy from a personalization program have less system-specific privacy concerns and are more likely to use it as a privacy tool [30]. Thus, the study concludes that having a good response efficacy would enable lower data loss.

5) Rewards (R): A study by [31] found that users reported getting a lot of credit on SNSs when a lot of personal information being posted. From previous research, rewards are described as receiving attention and response from posting on SNSs through like comments and "likes". However, implementing restrictive privacy settings can be a barrier to achieving certain rewards in SNSs [32]. Furthermore, users in SNSs trade their privacy information for gaining rewards in SNSs and obtain benefits such as popularity and enjoyment when disclosing personal information [33]. Once users experience the benefits of SNSs, they will choose to share their personal information to obtain these benefits [22]. Because those might give a negative impact on users as they desire to gain those rewards [34], users need to maximize the rewards derived from SNSs interactions with their contacts with privacy protection behavior within SNSs [35].

B. Hyperpersonal Communication Theory

Hyperpersonal Communication Theory (HCT) provides a model for understanding how users perceive emotional intimacy in computer-mediated communication (CMC)[36]. HCT provides more manageable online interaction, as information senders can cleverly select what and how to reveal [37]. Moreover, according to the concept of HCT, users had balanced their desires that sometimes competing for privacy with their willingness to be open in the SNSs environment and communicate with others. Previous research stated that the level and period of online messages could compensate and resulting in hyperpersonal communication or relationships that exceed face to face in terms of their emotional connection [36]. Hence, HCT identified that users of CMC are best able to discover their goodness by selecting the medium that fits their unique social needs perfectly [38].

1) Perceived anonymity of self: The perceived anonymity of self can be defined as the extent to which a sender perceives the source of the message as anonymous and undefined [38]. For instance, any picture, video, or post by a blogger or user on SNSs, could expose information about their virtual identity. Some identity information can be identified by at least their real name or their picture, while other things like blurred picture and nickname may only provide limited information about the user. At some point, the world of SNSs reveals users' real social identities and leads to a healthy exchange of content, whereas perceived anonymity of self-decreases the ability of users to share information [39]. The researcher has also found that a higher degree of perceived anonymity on SNSs means less need to reveal self [40]. Another study stated that perceived anonymity of self-gave a lot kind of good result, but somehow there is a lot of kind of user in which there must be some users give the negative effect of perceived anonymity of self [41]. As supported by some studies, the positive effect of anonymity of self on SNSs is the successful method to protect private information and create a private identity [42].

2) Perceived anonymity of others: The perceived anonymity of others relates to the absence of identification information and details about the other user on SNSs [43]. If other users are known as anonymous, recognizing who they are or keeping them to account for their acts and personal views is unlikely and difficult for the individual. The other user may be more likely to post information and comments using an anonymous online identity [44] and it makes individual difficult to know about the other user's identity as if the user is bad or not. The consequences of anonymity of others are mirrored in the results of the dark side of the Internet's personalization, fraud, and fake information [45], so individuals could probably fall into trap of scam. The anonymity of others can also present as a negative role in the exchange of information in internet-based interpersonal communication [46], as it always happens that the users fake their identity to make themselves feel better to communicate in SNSs. The view is supported by Twitter research that states that a lot of anonymous users have shared and create bad content by tweeting compare to non-anonymous users [47].

3) Perceived intrusiveness: Another serious recent problem in SNSs studies was perceived intrusiveness [48]. Perceived intrusiveness refers to how often people experience an unwanted violation of their environment [49]. In other words, high willingness in experiencing threats can lead to more sensitivity and less perceived intrusiveness [50]. Intrusiveness is a psychological theory that endorses the concept of creating an imbalance between the independence of two parties and the self-rule to protect personal identity on SNSs [51]. For instance, users could feel intrusive by spam from other users, slander, sexual harassment, cyberbully,

advertisement, and many other intrusive things. This will create higher levels of perceived intrusiveness and therefore more negative emotions for people who are particularly anxious with privacy when presenting themselves than seeing others [52].

In order to better understand the reason for students to adopt privacy protection behavior in SNSs, there is a need to determine the factors of their adoption. The proposed framework shown in this study was constructed based on PMT for perceived severity, perceived vulnerability, self-efficacy, response efficacy and rewards. Besides that, three variables from HCT including perceived anonymity of self, perceived anonymity of others and perceived intrusiveness is also included as determinants of privacy protection behavior.

This study combines PMT and HCT because PMT is a basic theory that is often used in research related to privacy protection behavior while HCT is the theory that offers an approach to understand how users experience relational intimacy in computer mediated communication (CMC) [36]. The combination of these two theories with the addition of variables from HCT can add value to existing studies as it focuses more on computer-mediated communication.

C. Privacy Protection Behavior

Privacy protection refers to the management of personal information disclosure while deflecting unwanted intrusions [53]. Protecting privacy behavior in this modern era is a must since it makes users concern about how the data shared is being stored or collected, also how the data being exposed to others when the user shared it. SNSs users may protect their privacy by not exposing too much about themselves, learn how to limit the privacy information that they share and exchange also by taking security steps for privacy [54]. When individuals feel betrayed, sense of unfairness, inequality, and emotional distress, they would then adopt various privacy protection to protect their privacy [55]. Hence, there is a need to find out more about how users use privacy protection, so the outcomes of their actions can be determined.

Privacy protection refers to an action that individuals perform to keep their information safe and been categorized into two categories namely: i) approach strategies and ii) avoidance strategies [56]–[58]. Approach strategies refer to confrontation strategies that encompass problem-solving and seeking social support while avoidance strategies are withholding and refusing to provide the information. Some approach strategies including fabricating personal information and seeking social support by asking for information and advice or reading the privacy statement. An example of avoidance strategies is removing or deleting offending people in SNSs, using privacy settings provided by SNSs, choose and control who can see their profiles and their posts, and with whom they can share their personal information. The use of such privacy strategies is important so that they can make informed decisions about sharing their information in desired ways. Besides, the use of privacy setting can help SNSs users to reap the benefits from selectively sharing content on SNSs, while at the same time minimizing the potential damage and harm to their reputation and relationships that may result from unintentional disclosures [59].

This paper proposes the theoretical framework as shown in Fig. 1. Essentially, this study re-examines the constructs as privacy protection factors concerning information sharing in SNSs setting. Based on the previous discussions, the following hypotheses are proposed:

H1: Perceived severity positively influenced privacy protection behavior in SNSs.

H2: Perceived vulnerability positively influenced privacy protection behavior in SNSs.

H3: Self-efficacy positively influenced privacy protection behavior in SNSs.

H4: Response efficacy positively influenced privacy protection behavior in SNSs.

H5: Rewards positively influenced privacy protection behavior in SNSs.

H6: Perceived anonymity of self positively influenced privacy protection behavior in SNSs.

H7: Perceived anonymity of others positively influenced privacy protection behavior in SNSs.

H8: Perceived intrusiveness positively influenced privacy protection behavior in SNSs.

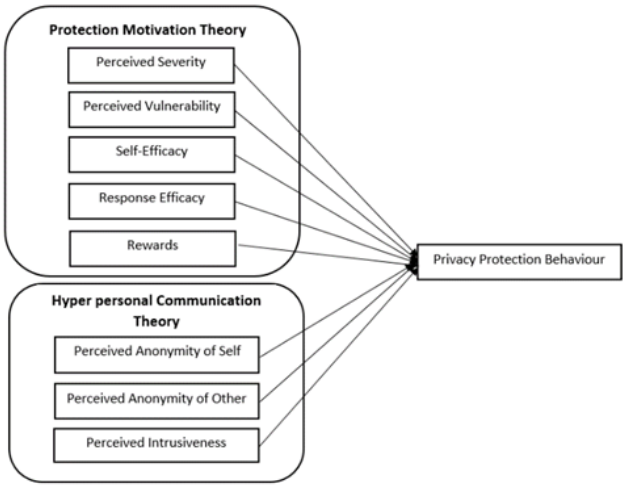

Fig. 1. Proposed Framework.

IV. Methodology

This section describes the details of the quantitative methodology adopted in the study.

A. Research Instrument Design

This study will use the survey questionnaire as the research instrument design. To detect any possible issues, the draft instruments were proposed to select experts in the field related. The aim is to remove any confusing or ambiguous words from the questionnaire, also help to improve questionnaire quality and reliability. Additionally, the

questionnaire was designed to be easily followed and respond to reduce sampling errors and to have a high number of respondents that voluntarily answer the questionnaire.

To develop a questionnaire, it is necessary to identify the variables. Questions are formulated depending on the appropriateness of the variables. Every defined variable consists of approximately ten items. To calculate the number of elements, the Likert scale is used as the method. The function of the Likert scale is to allow individuals to show an agreement level on a particular statement with a five-point scale. The scale used for topical value variable is 1 being "Strongly Disagree", 2 being "Disagree," 3 being "Neutral," 4 being "Agree" and 5 as "Strongly Agree". The questionnaire was divided into three sections, which are Section A for Demographic Information, Section B for Privacy Protection Behavior, and Section C for determinants that motivate Privacy Protection Behavior.

B. Content Validity

The aim of validating the content is to identify the items which represent the variable in the generated questionnaire. To conduct validation, selected experts will be given the form of content validation as annexed in the appendix. Three information security experts were involved in the testing of this study. The experts were selected based on their computer security expertise, with at least five to twenty years' experience in the field related to the study. The content validation of the research instrument was statistically analyzed using a Content Validation Index (CVI). CVI was stated as the higher common approach apply to quantitatively measure the validity of the content. In this validation case, it has two types of CVI, which is Item-CVI (I-CVI) and Scale-CVI (S-CVI). Simply described I-CVI is the total agreed rated by experts while S-CVI will be the average of total I-CVI. Thus, the item rated less than 1.00 in I-CVI, the item will be excluded from the set of questionnaires and the S-CVI must be higher than 0.90 for the variable of the item validated.

The result in Table I shows that two items in PPB, PS, SE, and PI were removed, three items in PV, one item in RE and PAO, four items in R, and no items were removed in PAOS and IPC. The total number of items removed was 17 and 54 items were retained in the questionnaire.

C. Data Collection

For the data collection, the target respondent as a sample of the population is high school students in Malaysia who are the users of SNSs. The questionnaire on the survey instrument is circulated online, using the Google Form. Using shared links through an online platform and social media, the questionnaire will be distributed through SNSs such as Whatsapp, Instagram, and Telegram. The data collection is completed in two weeks. All answers are gathered and recorded before analyzing the results.

The sampling method that is used for data collection is non-proportional quota sampling. This study target 200 respondents from different schools with computer courses, the age range are 16 to 19 years old. To take part in this study a total of 230 respondents must be chosen. From a total of 230 respondents, the first 30 respondents were involved in pilot tests and will be excluded from the main study. The remaining 200 respondents will go to the actual survey. To maximize accuracy, students who registered on at least one SNSs were determined to select the students to be involved in this study. Those who had no SNSs accounts would not be included in the study sample.

D. Reliability

Reliability was achieved by analyzing the items from the pilot test result and obtain the Cronbach's Alpha value. The value of Cronbach's Alpha was determined based on the pilot test result. The general Cronbach's Alpha value should be higher than 0.70. The higher the score the greater the reliability of the scale produced. For Section B, variable privacy protection behavior shows a result of 0.742 which means the internal consistency is respectable. Besides that, Section C contains 9 variables which show the coefficient alpha result as follows: perceived severity (0.814), perceived vulnerability (0.800), self-efficacy (0.810), response efficacy (0.891), perceived anonymity of self (0.857), and perceived intrusiveness (0.847). The results with an alpha value above 0.8 mean the internal consistency is very good. The results with an alpha value above 0.90 mean the internal consistency is excellent: rewards (0.917), perceived anonymity of others (0.925), and information privacy concern (0.934). Hence, overall from this pilot study, the questionnaire was tested as suitable for actual study in this research. No variable needs to be removed for the actual study. Table II shows the results of Cronbach's Alpha value.

TABLE I. CVI RESULTS

Variable	S-CVI (Before)	S-CVI (After)
PPB	0.906	1.00
PS	0.906	1.00
PV	0.810	1.00
SE	0.906	1.00
RE	0.945	1.00
R	0.624	1.00
PAOS	1.00	1.00
PAO	0.953	1.00
PI	0.890	1.00

TABLE II. RESULTS OF CRONBACH'S ALPHA VALUE

Section	Sub-Construct	Alpha
B	Privacy Protection Behavior	0.742
C	Perceived Severity	0.814
	Perceived Vulnerability	0.800
	Self-Efficacy	0.810
	Response Efficacy	0.891
	Rewards	0.917
	Perceived Anonymity of Self	0.857
	Perceived Anonymity of Others	0.925
	Perceived Intrusiveness	0.847

V. Results

In this section, the result obtained from the survey will be analyzed through a few analyses.

A. Factor Analysis

In this study, Principal Component Analysis is used to perform construct validity. During the analysis, the items with low load factor values will be removed as it was considered as problematic. In this study, it had been set a higher cut-off value of 0.6 for loading factors [60]. The items removed were 8 items which are PAOS1, PAOS2, PAOS3, PAOS4, PAO1, PAO2, PAO3, and PI3 with factor loadings of less than 0.6. Factors that contain less than 3 items are counted as useless and weak, so it must be eliminated [61]. In this case, there is no factor in less than 3 items, hence, no factor will be removed. The final analysis shows that 41 items were retained. Also, two factors fall under the same number of the component which is number 4, PAOS and PAO. Both of the factors were a different factor but were combined under one factor. PAOS is the individual being anonymous in SNSs while PAO is another user being anonymous in SNSs. Assuming that, high school student believes that it is no difference between both of the factor, either themselves of other user being anonymous in SNSs might help in protecting the privacy. By being anonymous, they could implement privacy protection behavior. Therefore, in this case, both of them were combined under one factor namely PA (Perceived Anonymity). Table III shows the results of the factor analysis.

TABLE III. Results of Factor Analysis

Item	1	2	3	4	5	6	7
PS1				.715			
PS2				.787			
PS3				.688			
PS4				.678			
PS5				.723			
PV1					.690		
PV2					.786		
PV3					.871		
PV4					.851		
SE1		.692					
SE2		.798					
SE3		.720					
SE4		.723					
SE5		.749					
RE1	.737						
RE2	.771						
RE3	.658						
RE4	.808						
RE5	.824						
R1						.729	
R2						.894	
R3						.861	
R4						.659	
PAOS5			.714				
PAOS6			.660				
PAOS7			.662				
PAO4			.722				
PAO5			.578				
PAO6			.660				
PI1							.697
PI2							.695
PI4							.675

B. Regression Analysis

Multiple regression analysis is conducted to estimate the relationship between some of the independent variables towards a dependent variable. Multiple regressions were run in this study and the results are shown in Table IV. The results of multiple regression analysis showed that six independent variables, i.e. perceived severity, perceived vulnerability, self-efficacy, response efficacy, perceived anonymity, and perceived intrusiveness significantly influenced the dependent variable which is privacy protection behavior. However, H5 was not supported in this study. Based on the result obtained, the model that predicts the motivational determinants of privacy protection behavior were identified. The β value shows the strength of the relationship, the higher the β value the stronger the relationship. R square for this regression model was 0.331, which indicated 33.1% of the variance in privacy protection behavior is explained by perceived severity, perceived vulnerability, self-efficacy, response efficacy, perceived anonymity, and perceived intrusiveness. Further examination on the standardized beta coefficient revealed that the most dominant factor that affects the respondents' privacy protection behavior was perceived anonymity (β = .378), followed by perceived intrusiveness (β = .277), perceived severity (β = .264), self-efficacy (β = .227), perceived vulnerability (β = .210) and response efficacy (β = .209).

TABLE IV. Results of Multiple Regression

Model	Standardized Coefficients	*t*	*Sig.*
	Beta (β)		
PS → PPB	.264	3.977	.000
PV → PPB	.210	3.360	.001
SE → PPB	.227	3.202	.002
RE → PPB	.209	3.229	.001
R → PPB	.095	1.499	.135
PA → PPB	.378	5.946	.000
PI → PPB	.277	4.352	.000
Notes: Overall Model F= 48.334; $p<0.05$; $R^2 = 0.331$; adjusted $R^2 = 0.34$			

VI. Discussion

From the factor analysis, a few items were removed because of the low load factor as it was considered problematic. Also, two variables were merged into one factor namely Perceived Anonymity as it measures the same thing which is Perceived Anonymity of Self and Perceived Anonymity of Other. From these results, we can assume that high school students believed that anonymity does not matter, whether, on their side or the side of others, does help to keep their personal information safe.

As for the result of regression analysis, the potential of motivational determinants was perceived severity, perceived vulnerability, self-efficacy, response efficacy, perceived anonymity, and perceived intrusiveness and it was determined as positively influenced with privacy protection behavior. The determinants do motivate high school students to implement privacy protection behavior. Perceived anonymity was found

to be the highest determinant of privacy protection behavior. This result shows that the students highly agreed that even if they try to hide their identity, their privacy can still be disturbed. In SNSs, even if users try to conceal their identity using nicknames or images that do not show their identity, other users might be able to guess their identity based on their mutual friends. Besides, students are also motivated to adopt protective action when confronted with strangers or anonymous people on SNSs. This is perhaps when others decline to expose their identification, students find it difficult to get enough factual information to better understand others. Unknown individuals might have bad intentions. Hence, it motivates students to adopt privacy protection behavior on SNSs even if the identity is anonymous.

VII. Conclusion

The main purpose of this research is to study the potential motivational determinants of privacy protection behavior. A model for the privacy protection behavior in SNSs is proposed by defining the main elements and provide a comprehensive model that will motivate the high school students in implementing privacy protection behavior. The results of this study are expected to be used to increase the level of privacy protection behavior among all users in SNSs and also to build up privacy guidelines. This study could motivate and influence the user to implement privacy protection behavior when utilizing SNSs.

Financial and time constraints limit the selection of the population in this study. However, the generalization for this study can be applied to the level of all students who have similar characteristics. The recommendation for future study in this field could overcome the limitation of this study such as the method to collect data by using quota sampling. This could be overcome by using a probability sampling method that could avoid bias selection on the population. The method of collecting the feedback from the respondent by using a questionnaire also could be improved in a future study to gain more variety of feedback such as interview, recording, observation, and others. A better and specific study to gain more understanding of privacy protection behavior can be obtained using qualitative analysis. Besides, this study could be improved by adding more motivational determinants towards privacy protection behavior. There could be more potential motivational determinants to exert more significant influence and impact on privacy protection behavior. Last but not least, expanding sample size and other ages with their background of education or various experience of the respondent can be extended to better generalize the analysis and potentially strengthen it among users of SNSs in Malaysia. By expanding sample size and age with educational background or experience, it may result in different intend, patterns, and behavior in SNSs. Hence, the future study can overcome all the limitations in this study to gain better and specific results of privacy protection behavior among SNSs users in Malaysia.

Acknowledgment

The authors would like to thank Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka (UTeM) for supporting the work done in this paper.

References

[1] Kassim, P.N.J., 2008. The Development of e-Health in Malaysia: New Challenges to the Healthcare Industry.

[2] Zilles, M., 2011. Online Social Networks in Germany: Privacy Behaviour and Concern.

[3] S. Encrypt, “What is Privacy Protection? [Updated for 2020],” Search Encrypt Blog, Dec. 20, 2019.

[4] Van den Hoven, Jeroen, et al. “Privacy and Information Technology.” The Stanford Encyclopedia of Philosophy, edited by Edward N. Zalta, Summer 2020.

[5] M. Micheli, C. Lutz, and M. Büchi, “Digital Footprints: An Emerging Dimension of Digital Inequality,” Journal of Information Communication and Ethics in Society, vol. 16, pp. 242–251, Jun. 2018.

[6] R. Robinson, “Data Privacy vs. Data Protection,” Jan. 30, 2020.

[7] F. O., “Social Networking Privacy Concerns Impacting Businesses and Consumers,” Security Boulevard, N, 2019.

[8] Shanthi Kandiah, “Malaysia - The Privacy, Data Protection and Cybersecurity Law Review - Edition 6 - TLR - The Law Reviews,” Oct. 2019.

[9] Royce Tan and Sharmila Nair "M’sia sees biggest mobile data breach", NATION, Tuesday, 31 Oct 2017.

[10] Khairani Afifi Noordin, “News: Protect yourself from identity theft,” The Edge Markets, Nov. 21, 2017.

[11] Bernama, 2015. Laman Sosial Bukan Diari Peribadi. Malaysian Communication and Multimedia Commission. Available at: http://www.skmm.gov.my/Media/Press-Clippings/Laman-Sosial-Bukan-Diari-Peribadi-SKMM.aspx?lang=en-US.

[12] Malaysia Computer Emergency Report Team (MyCERT), 2020. Reported Incidents based on General Incident Classification Statistics 2019. Available at: https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169 66677d694932&id=0d39dd96-835b-44c7-b710-139e560f6ae0

[13] S. C. Boerman, S. Kruikemeier, and F. J. Zuiderveen Borgesius, “Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data,” Communication Research, Oct. 2018.

[14] L. Baruh, E. Secinti, and Z. Cemalcilar, “Online Privacy Concerns and Privacy Management: A Meta-Analytical Review,” J Commun, vol. 67, no. 1, pp. 26–53, Feb. 2017.

[15] M. Büchi, N. Just, and M. Latzer, “Caring is not enough: the importance of Internet skills for online privacy protection,” Information, Communication & Society, vol. 20, no. 8, pp. 1261–1278, Aug. 2017.

[16] M. C. Green, “Social Network Sites and Well-Being: The Role of Social Connection,” Curr Dir Psychol Sci, vol. 27, no. 1, pp. 32–37, Feb. 2018.

[17] B. Palladino et al. and E. Menesini et al., “Perceived Severity of Cyberbullying: Differences and Similarities across Four Countries,” Frontiers in Psychology, vol. 8, p. 1524, Sep. 2017.

[18] K. Adhikari and R. K. Panda, “Users’ Information Privacy Concerns and Privacy Protection Behaviors in Social Networks,” Journal of Global Marketing, vol. 31, no. 2, pp. 96–110, Mar. 2018.

[19] T. Wang, T. D. Duong, and C. C. Chen, “Intention to disclose personal information via mobile applications: A privacy calculus perspective,” International Journal of Information Management, vol. 36, no. 4, pp. 531–542, Aug. 2016.

[20] B. Hanus and Y. Wu, “Impact of Users’ Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective,” Information Systems Management, vol. 33, Nov. 2015.

[21] S. Jain and S. Agrawal, “Perceived vulnerability of cyberbullying on social networking sites: effects of security measures, addiction and self-disclosure,” Indian Growth and Development Review, vol. ahead-of-print, Jun. 2020.

[22] M. Abdul Hameed and N. Arachchilage, “On the Impact of Perceived Vulnerability in the Adoption of Information Systems Security Innovations,” International Journal of Computer Network and Information Security, vol. 11, pp. 9–18, Apr. 2019.

[23] X. Zhang, S. Liu, X. Chen, L. Wang, B. Gao, and Q. Zhu, "Health information privacy concerns, antecedents, and information disclosure intention in online health communities," Information & Management, vol. 55, no. 4, pp. 482–493, Jun. 2018.

[24] F. Mwagwabi, T. McGill, and M. Dixon, "Short-term and Long-term Effects of Fear Appeals in Improving Compliance with Password Guidelines," Communications of the Association for Information Systems, pp. 147 – 182, Feb. 2018.

[25] M. Vatka, "Information Behavior And Data Security : Health Belief Model Perspective," 2019.

[26] N. Arachchilage, "User-Centred Security Education: A Game Design to Thwart Phishing Attacks," Nov. 2015.

[27] R. Fida, C. Tramontano, M. Paciello, Valerio Ghezzi, and C. Barbaranelli, "Understanding the Interplay Among Regulatory Self-Efficacy, Moral Disengagement, and Academic Cheating Behavior During Vocational Education: A Three-Wave Study," Journal of Business Ethics, vol. 153, Dec. 2018.

[28] K. D. Martin, A. Borah, and R. W. Palmatier, "Data Privacy: Effects on Customer and Firm Performance," Journal of Marketing, vol. 81, no. 1, pp. 36–58, Jan. 2017.

[29] H. Lee and A. Kobsa, "Understanding user privacy in Internet of Things environments," in 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, Dec. 2016, pp. 407–412.

[30] T. Dienlin and M. J. Metzger, "An Extended Privacy Calculus Model for SNSs: Analyzing Self-Disclosure and Self-Withdrawal in a Representative U.S. Sample," Journal of Computer-Mediated Communication, vol. 21, no. 5, pp. 368–383, 2016.

[31] D. Wang, "A study of the relationship between narcissism, extraversion, body-esteem, social comparison orientation and selfie-editing behavior on social networking sites," Personality and Individual Differences, vol. 146, pp. 127–129, Apr. 2019.

[32] H.-T. Chen and W. Chen, "Couldn't or Wouldn't? The Influence of Privacy Concerns and Self-Efficacy in Privacy Management on Privacy Protection," Cyberpsychology, behavior and social networking, vol. 18, pp. 13–9, Jan. 2015.

[33] N. Park and Y.-J. Kim, "The Impact of Social Networks and Privacy on Electronic Word-of-Mouth in Facebook: Exploring Gender Differences," 2020.

[34] Craig R.Scott, "To Reveal or Not to Reveal: A Theoretical Model of Anonymous Communication," Commun Theory, vol. 8, no. 4, pp. 381–407, Nov. 1998.

[35] Z. Liu, Q. Min, Q. Zhai, and R. Smyth, "Self-disclosure: A social exchange theory perspective," Information & Management, vol. 53, no. 1, pp. 53–63, Jan. 2016.

[36] E. Sumner and A. Ramirez, "Social Information Processing Theory and Hyperpersonal Perspective," 2017.

[37] J. Mou and D. Shin, "Effects of social popularity and time scarcity on online consumer behavior regarding smart healthcare products: An eye-tracking approach," Computers in Human Behavior, vol. 78, pp. 74–89, Jan. 2018.

[38] T. L. Cigelske, "The Highest Form of Like: Snapchat, College Students and Hyperpersonal Communication," undefined, 2018.

[39] X. Chen, M. Sun, D. Wu, and X. Y. Song, "Information-Sharing Behavior on WeChat Moments: The Role of Anonymity, Familiarity, and Intrinsic Motivation," Front. Psychol., vol. 10, 2019.

[40] C. P. Barlett, D. A. Gentile, and C. Chew, "Predicting cyberbullying from anonymity.," Psychology of Popular Media Culture, vol. 5, no. 2, pp. 171–180, Apr. 2016.

[41] X. Lin, M. Featherman, and S. Sarker, "Understanding factors affecting users' social networking site continuance: A gender difference perspective," Information & Management, vol. 54, no. 3, pp. 383–395, Apr. 2017.

[42] L. Levontin and E. Yom-Tov, "Negative Self-Disclosure on the Web: The Role of Guilt Relief," Frontiers in Psychology, vol. 8, Jun. 2017.

[43] H. Nissenbaum, "The Meaning of Anonymity in an Information Age," The Information Society, vol. 15, no. 2, pp. 141–144, May 1999.

[44] E. Jardine, "The Dark Web Dilemma: Tor, Anonymity and Online Policing," Global Commission on Internet Governance Paper Series, p. 24, Sep. 2015.

[45] J. Fox and J. J. Moreland, "The dark side of social networking sites: An exploration of the relational and psychological stressors associated with Facebook use and affordances," Computers in Human Behavior, vol. 45, pp. 168–176, 2015.

[46] J. D. Morris, Y. Choi, and I. Ju, "Are Social Marketing and Advertising Communications (SMACs) Meaningful?: A Survey of Facebook User Emotional Responses, Source Credibility, Personal Relevance, and Perceived Intrusiveness," Journal of Current Issues & Research in Advertising, vol. 37, no. 2, pp. 165–182, Jul. 2016.

[47] J. Burgoon, R. Parrott, B. Poire, D. Kelley, J. Walther, and D. Perry, "Maintaining and Restoring Privacy Through Communication in Different Types of Relationships," Journal of Social and Personal Relationships - J SOC PERSON RELAT, vol. 6, pp. 131–158, May 1989.

[48] N. A. Dodoo and J. (Taylor) Wen, "Weakening the avoidance bug: The impact of personality traits in ad avoidance on social networking sites," Journal of Marketing Communications, vol. 0, no. 0, pp. 1–24, Jan. 2020.

[49] V. M. Wottrich, E. A. van Reijmersdal, and E. G. Smit, "App Users Unwittingly in the Spotlight: A Model of Privacy Protection in Mobile Apps," Journal of Consumer Affairs, vol. 53, no. 3, pp. 1056–1083, 2019.

[50] Y. Feng and Q. Xie, "Privacy Concerns, Perceived Intrusiveness, and Privacy Controls: An Analysis of Virtual Try-On Apps," Journal of Interactive Advertising, pp. 1–41, Sep. 2018.

[51] C. Goodwin, "A Conceptualization of Motives to Seek Privacy for Nondeviant Consumption," J. Consum. Psychol., vol. 1, no. 3, pp. 261–284, 1992.

[52] M. Qi and D. Edgar-Nevill, "Social networking searching and privacy issues," Inf. Secur. Tech. Rep., vol. 16, no. 2, pp. 74–78, 2011, doi: 10.1016/j.istr.2011.09.005.

[53] B. C. F. Choi, Z. Jiang, B. Ramesh, and Y. Dong, "Privacy tradeoff and social application usage," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 2015-March, pp. 304–313, 2015, doi: 10.1109/HICSS.2015.44.

[54] Y. Feng and W. Xie, "Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors," Comput. Human Behav., vol. 33, no. July, pp. 153–162, 2014, doi: 10.1016/j.chb.2014.01.009.

[55] B. C. F. Choi, Z. Jiang, B. Ramesh, and Y. Dong, "Privacy tradeoff and social application usage," Proc. Annu. Hawaii Int. Conf. Syst. Sci., vol. 2015-March, pp. 304–313, 2015, doi: 10.1109/HICSS.2015.44.

[56] E. G. Smit, G. Van Noort, and H. a. M. Voorveld, "Understanding online behavioral advertising: User knowledge, privacy concerns and online coping behavior in Europe," Comput. Human Behav., vol. 32, pp. 15–22, Mar. 2014, doi: 10.1016/j.chb.2013.11.008.

[57] E. Litt, "Understanding social network site users' privacy tool use," Comput. Human Behav., vol. 29, no. 4, pp. 1649–1656, 2013, doi: 10.1016/j.chb.2013.01.049.

[58] Tu, Z., Turel, O., Yuan, Y. & Archer, N., 2015. Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. Information and Management, 52(4), pp.506–517.

[59] F. Banhawi, N. Mohamad Ali, and H. Judi, "User engagement attributes and levels in Facebook," Journal of Theoretical and Applied Information Technology, vol. 15, Jan. 2012.

[60] R. Maskey, J. Fei, and H.-O. Nguyen, "Use of Exploratory Factor Analysis in Maritime Research," The Asian Journal of Shipping and Logistics, vol. 34, no. 2, Art. no. 2, 2018.

[61] T. W. MacFarland and J. M. Yates, Introduction to Nonparametric Statistics for the Biological Sciences Using R. Springer International Publishing, 2016.