


Determinants of the Intention to Protect Personal Information among Facebook Users

Bum Soo Chon , Jeong-Ki Lee, HyeonJu Jeong, Jowon Park, and Jonghwa Park

This study aimed to examine predictors of the intention to protect personal information on Facebook. We conducted an online survey of 679 Facebook users in the Republic of Korea. The findings of this study showed that usefulness and ease of use had significant effects on attitudes toward protection behavior. The results also revealed that risk factors (privacy risk severity and vulnerability) had significant effects on protective behaviors. Based on our findings, we discussed the information protection of privacy on Facebook.

Keywords: Facebook, Information protection, Intention to protect personal information, SNS privacy.

I. Introduction

Social network services (SNS) such as Facebook make it possible to expand one's relationships with others for a variety of reasons [1]. The widespread availability of smartphones has accelerated the use of SNSs; this allows individuals to use SNSs regardless of time and space, and therefore, SNSs have become major communication channels. The growth of SNSs has threatened users in a variety of ways, including privacy issues. Most SNS users disclose their information; however, such disclosed information can be exploited for commercial purposes without consent [2]. Thus, the privacy issue in SNSs has been a major research topic in recent years [3].

Although SNSs help individuals maintain their social relationships, the disclosure of personal information required to maintain and expand these relationships on SNSs is concerning [1], [3]. This disclosure can increase the possibility of an invasion of privacy on social networks. Users' desire for self-expression can lead to revealing a significant amount of personal information on SNS, and such self-disclosure may cause unwanted consequences such as identity theft [4]. Thus, many researchers have investigated privacy issues in SNSs. Nevertheless, there is no comprehensive framework that explains this issue.

The purpose of this study was to identify the determinants of the intention to protect personal information among Korean Facebook users. More specifically, this research investigated structural and sociopsychological attributes that may explain the intention to protect personal information based on three theories: the technology acceptance model (TAM), theory of planned behavior (TPB), and protection motivation theory (PMT). Based on these theories, this paper explored the relationships between variables of TAM,

Manuscript received Apr. 2, 2017; revised Oct. 16, 2017; accepted Oct. 30, 2017.

Bum Soo Chon (corresponding author, bumchon@naver.com) and Jowon Park (parkjowon@hanyang.ac.kr) are with the Department of Journalism & Communication, Hanyang University, Ansan, Rep. of Korea.

Jeong-Ki Lee (jkl8181@hanyang.ac.kr) is with the Center for Teaching & Learning, Hanyang University, Seoul, Rep. of Korea.

HyeonJu Jeong (dally12kr@naver.com) is with the Department of Advertising and Public Relations, Catholic Kwandong University, Gangneung, Rep. of Korea.

Jonghwa Park (bjh0515@unist.ac.kr) is with the School of Management Engineering, Ulsan National Institute of Science and Technology, Rep. of Korea

This is an Open Access article distributed under the term of Korea Open Government License (KOGL) Type 4: Source Indication + Commercial Use Prohibition + Change Prohibition (<http://www.kogil.or.kr/info/licenseTypeEn.do>).

TPB, and PMT that predict the intention to protect personal information on Facebook.

II. Literature Review

Davis [5] developed the TAM, which is an extension of the theory of reasoned action (TRA) [6]. The premise of TRA was that human behavior is rational. According to TRA, human behavior can be predicted from attitude (which can be defined as positive or negative cognition as a personal factor) and subjective norm (which is defined as a person's perceptions of how others judge a behavior as a social factor) [7]. By contrast, according to TAM, a person's behavior using a new technology or service can be predicted from perceived usefulness (which is the perception of whether using a new technology will improve his or her work) and perceived ease of use (which is the perception of whether using a new technology will be free of effort).

TRA is the basis for TAM in that the decision to accept a new technology depends on the expectancy-value theory [8]. TAM is the refined conceptual model of TRA for explaining the process of new technology acceptance [9]. TAM has been widely applied to predict acceptance behavior toward various forms of new media. For example, TAM was used to estimate the intention to use e-mail [10] and SNSs [11].

The TPB, developed by Azjen [12], was also derived from TRA. TRA takes account of personal and social factors simultaneously to explain the possibility of performing specific behavior. However, some critics suggested that the theory lacked the concept of efficacy, which is the belief that a behavior can be conducted based on one's own will. In TPB, therefore, perceived behavioral control was added to TRA with attitude and a subjective norm.

TPB is useful in explaining and predicting sociocultural aspects of behavioral intention. More specifically, it can help predict information-security-related behavioral intention such as the intention to follow policies for information system security [13] and comply with information security policy [14].

Recently, there have been vigorous attempts to fuse TPB with other theoretical frameworks such as TAM in order to increase the explanatory power of the sociocultural approach to human behavior. For example, Lu and others [15] utilized an integrated model of TAM and TPB to predict the intention to use Messenger. They showed that ease of use had a positive effect on usefulness, and usefulness had a positive effect on attitude and the behavioral intention to use Messenger. They

demonstrated that attitude, subjective norm, and perceived behavioral control all had positive influences on behavioral intention. The integrated model of the two theories also showed a stable fit index.

In addition, Lee [16] showed that this integrated model displayed a stable fit index in predicting the intention to use Internet banking. Specifically, TAM variables including perceived ease of use and perceived usefulness had positive effects on attitudes toward Internet banking use, and perceived usefulness had a positive effect on the intention to use Internet banking. Moreover, TPB variables of attitude, subjective norm, and perceived behavioral control had positive effects on the intention to use Internet banking.

The above results demonstrated that the integrated TAM-TPB model had a stable fit index and higher explanatory power in predicting users' technology-based behavioral intention than the use of only a single model. Therefore, the current study employed the integrated TAM-TPB model to predict technology-based behavioral intention in the context of personal information protection on Facebook.

The PMT, proposed by Rogers [17], provides a social psychological perspective on the health-related belief model. PMT is useful in predicting attitude changes under fear appeals. PMT has been considered a powerful theory for predicting protection-related behavioral intention [18].

Additionally, PMT has been used to predict behavioral intention for health protection in the realm of health communication [19], and to predict behavioral intention in the context of information protection [20]-[22]. For example, Lee [20] examined the usefulness of PMT variables in predicting the intention to adopt anti-plagiarism software. Lee and Larsen [21] also presented an empirical investigation to explain factors affecting the adoption of anti-malware software based on PMT.

Moreover, Mohamed and Ahmad [22] attempted to explain information privacy concerns by investigating their antecedents and privacy measures in an SNS context. The results showed that perceived vulnerability, self-efficacy, and perceived severity affected the information privacy concerns of social networking sites, and that high privacy concern can provoke active use of the privacy policy established by the SNS provider. These research results demonstrate that PMT is useful in predicting users' intentions to protect their privacy on SNSs.

In a study integrating PMT and TPB, Ifinedo [13] found that vulnerability had a positive effect, and severity had a negative effect, on the intention to comply with information system security policies. The integrated model exhibited a 70% explanatory power in predicting

behavioral intention, which indicates the usefulness of the integrated TPB–PMT model. Despite its advantages, there is a lack of studies about the integrating model. Accordingly, the current study seeks to maximize the explanatory power in explaining and predicting behavioral intention to protect personal information on Facebook by using a model that integrates TAM, TPB, and TAM.

III. Research Framework

1. Research Question

To examine the determinants of the intention to protect personal information on Facebook, the present study applied a model integrating three theories: TAM, TPB, and PMT. Although we employed TAM to examine individuals' adoption of technology-based services, we utilized TPB to examine the sociocultural aspects of user adoption. Additionally, PMT was included in our model in order to encompass cognitive processes under threatening conditions. More specifically, we employed relevant key factors from each model: perceived usefulness, perceived ease of use, and intention to use from TAM; attitude, subjective norm, and perceived behavioral control from TPB; and severity and vulnerability from PMT. Thus, our research question is, "What structural relationships do the key factors have regarding the protection of personal information on Facebook?"

2. Data Collection

In this study, respondents were selected based on quota sampling depending on gender and age through an online survey company. The survey was conducted for 10 days, February 15 through February 25, 2014, with Facebook users. There were 679 respondents in total, aged 10 to 50 years, and consisting of 335 males (49.3%) and 344 females (50.7%). Their age composition was as follows: 131 (19.3%) were 10 years old to 19 years old, 138 (20.3%) were in their 20s, 132 (19.5%) in their 30s, 136 (20.0%) in their 40s, and 142 (20.9%) in their 50s. The mean age was 34.98 ($SD = 13.41$) years. The mean Facebook usage time was 42.20 min, and the mean daily number of times that Facebook was accessed was 5.85.

3. Measurement

A. Perceived Usefulness

According to Venkatesh and Davis [23], perceived usefulness in the process of technology acceptance was

measured on a 5-point Likert scale indicating the level of agreement (1 = *strongly disagree*, 5 = *strongly agree*) with each of three items: "Setting personal information protection on Facebook is very useful in that it can securely protect personal information," "If you set personal information protection on Facebook, you can use Facebook more securely," and "Setting personal information protection on Facebook is effective in protecting personal information" ($M = 3.29$, $SD = 0.86$, $\alpha = 0.87$).

B. Perceived Ease of Use

Using Venkatesh and Davis' study [23], perceived ease of use in the process of technology acceptance was measured on a 5-point Likert scale indicating the level of agreement with the following statements: "Learning the way of personal information protection on Facebook is easy" and "The way of personal information protection on Facebook is clear and easy to understand" ($M = 3.18$, $SD = 0.79$, $\alpha = 0.89$).

C. Attitude

According to Ajzen's study [24], attitude, meaning the positive or negative perception of a particular behavior, was measured on a 5-point Likert scale indicating the level of agreement (1 = *strongly disagree*, 5 = *strongly agree*) with each of three items: "It is desirable to set the protection of personal information on Facebook," "I regard the behavior to set the protection of personal information on Facebook to be positive," and "Setting privacy protection on Facebook is a good idea" ($M = 3.84$, $SD = 0.78$, $\alpha = 0.92$).

D. Subjective Norm

Using Wang and McClung's variables [25], the subjective norm, which involves a person's evaluation of judgments made by important others, was measured on a 5-point Likert scale indicating the level of agreement with one item: "Most people who are important to me want me to protect my personal information on Facebook" ($M = 3.53$, $SD = 0.79$, $\alpha = 0.90$).

E. Perceived Behavioral Control

Based on Wang and McClung's study [25], perceived behavioral control, referring to the ability to control one's own behavior, was measured on a 5-point Likert scale with one item: "I can decide whether I set the protection of

personal information on Facebook of my own will” ($M = 3.71$, $SD = 0.80$, $\alpha = 0.84$).

F. Severity

Using Ifinedo’s study [13], severity was measured on a 5-point Likert scale indicating the level of agreement (1 = *strongly disagree*, 5 = *strongly agree*) with each of three items: “Having one’s privacy invaded on Facebook would harm one’s private life;” “The matter of privacy invasion on Facebook could paralyze social functions,” and “The problem of privacy invasion on Facebook may cause confusion in networks” ($M = 3.65$, $SD = 0.86$, $\alpha = 0.84$).

G. Vulnerability

According to Ifinedo’s study [13], vulnerability was measured on a 5-point Likert scale with three items: “I think data loss can happen to me when I use Facebook services,” “I think there is a possibility that somebody could collect information uploaded on the Facebook server without my permission,” and “Facebook’s system for protecting privacy is vulnerable” ($M = 3.72$, $SD = 0.76$, $\alpha = 0.82$).

H. Intention to Protect Personal Information

The dependent variable, the intention to protect personal information on Facebook, utilized items previously employed in studies by Ajzen [12] and Bulgurcu and others [14] studies. It was measured on a 5-point Likert scale with three items: “I will set the protection of personal information to maintain privacy during Facebook use,” “I will actively monitor whether my information is stolen to protect my private life,” and “I do not want to disclose personal information on Facebook” ($M = 3.76$, $SD = 0.72$, $\alpha = 0.77$).

4. Data Analysis

In this study, we sought to identify determinants of the intention to protect personal information on Facebook. To achieve this goal, we employed a model that integrated TAM, TPB, and PMT as the theoretical background. Specifically, this study examines the data fit of the integrated model regarding the independent variables, and identifies the structural relationship between all variables. For this purpose, we employed structural equation modeling through partial least squares (PLS). Smart PLS software (version 2.0), developed based on the

Java language at Hamburg University, was employed to estimate PLS path models. PLS is considered suitable for constructing an exploratory form of a cause-and-effect model [26].

IV. Results

1. Analysis of Reliability and Validity

We analyzed the reliability using the PLS algorithm in SmartPLS 2.0, examining Cronbach’s α and composite reliability. Table 1 lists the confirmatory factor analysis (CFA) results. The results showed that composite reliability is above the recommended minimum value of 0.7. Therefore, the reliability of measurement instruments was adequate. The reliability of the measurement model was also good, with a Cronbach’s α of more than 0.7.

Then, to satisfy the convergent validity of the measurement model, we examined factor loadings using CFA as well as average variance extracted (AVE). According to recommendations, when the CFA results show that the factor loadings for items are above 0.6, convergent validity is confirmed [27]. In the current study, the factor loadings of all measurement items were greater than 0.6. Therefore, there is no problem in the convergent validity of the measurement model. Meanwhile, the square root of the AVE can also evaluate convergent validity. AVE represents the shared variance of the latent variable and its measurement item. The greater the AVE, the larger the convergent validity. Generally, it is said that the convergent validity is good when AVE is above 0.5 [26], [27]. In the current study, the AVEs of all measurement items are greater than 0.6; thus, the convergent validity is acceptable.

Table 1. Results of CFA.

	AVE	Reliability	R Squared	Cronbach’s Alpha
EU	0.826	0.934	N/A	0.894
U	0.795	0.921	0.406	0.872
V	0.731	0.891	N/A	0.816
S	0.754	0.902	N/A	0.836
A	0.856	0.947	0.292	0.916
SN	0.831	0.937	N/A	0.898
PBC	0.754	0.902	N/A	0.837
IP	0.682	0.865	0.364	0.770

EU = Ease of Use, U = Usefulness, V = Vulnerability, S = Severity, SN = Subjective Norm, A = Attitude, PBC = Perceived Behavioral Control, IP = Intention to protect.

Table 2. Correlation coefficients and square root of AVE.

	IP	S	EU	U	SN	V	A	PBC
IP	0.826	N/A	N/A	N/A	N/A	N/A	N/A	N/A
S	0.037	0.868	N/A	N/A	N/A	N/A	N/A	N/A
EU	0.278	0.012	0.908	N/A	N/A	N/A	N/A	N/A
U	0.292	0.013	0.637	0.891	N/A	N/A	N/A	N/A
SN	0.455	0.037	0.325	0.353	0.911	N/A	N/A	N/A
V	0.405	0.067	0.081	0.065	0.307	0.854	N/A	N/A
A	0.531	0.034	0.309	0.387	0.628	0.386	0.924	N/A
PBC	0.356	0.026	0.418	0.395	0.437	0.271	0.549	0.868

Boldfaced letters represent the square root of AVE.

EU = Ease of Use, U = Usefulness, V = Vulnerability, S = Severity, SN = Subjective Norm, A = Attitude, PBC = Perceived Behavioral Control, IP = Intention to protect.

The discriminant validity of the measurement model can be evaluated by comparing the correlation coefficients of the latent variables and the square root of AVE. When the square root of AVE is greater than the correlation coefficient between two latent variables, the discriminant validity is considered good. The analysis showed that the square root of AVE was greater than the correlation coefficients (Table 2). The result indicated that all variables from TAM, TPB, and PMT have enough reliability and validity to test dependent variables with the intention to protect personal information on Facebook.

2. Path Analysis for Intention to Protect Personal Information on Facebook

To examine the intention to protect personal information on Facebook using TAM, TPB, and PMT, we conducted a bootstrapping test with Smart PLS. We set the number of samples for bootstrapping to 500, a default offered by Smart PLS. The findings from investigating the path that affects the intention to protect personal information on Facebook are shown in Table 3 and Fig. 1, and are described as follows.

First, the variables from TAM, usefulness ($\beta = 0.31$, $t = 2.18$, $p < 0.01$) and ease of use ($\beta = 0.28$, $t = 2.63$, $p < 0.01$), had positive impacts on the attitude toward protecting personal information on Facebook. In addition, ease of use had a positive effect on usefulness ($\beta = 0.64$, $t = 8.42$, $p < 0.001$). Of the TAM variables, however, only ease of use had a positive effect on the intention to protect personal information on Facebook ($\beta = 0.20$, $t = 1.74$, $p < 0.1$). Usefulness had indirect effects on the intention to protect personal information on Facebook through attitude.

These results indicated that perceptions of usefulness and ease of use with respect to protecting personal

Table 3. Path of factors affecting personal information protection on Facebook.

	Beta	M	STDEV	STERR	T
S → IP	0.110	0.129	0.126	0.126	0.878
S → A	0.077	0.084	0.120	0.120	0.639**
EU → IP	0.198	0.189	0.114	0.114	1.738 [†]
EU → U	0.637	0.637	0.075	0.076	8.420***
EU → A	0.275	0.264	0.105	0.105	2.629**
U → IP	0.143	0.143	0.118	0.118	1.214
U → A	0.305	0.309	0.140	0.140	2.183**
SN → IP	0.132	0.130	0.127	0.127	1.038
V → IP	0.270	0.257	0.129	0.129	2.088*
V → A	0.314	0.318	0.124	0.124	2.530*
A → IP	0.303	0.294	0.148	0.148	2.046*
PBC → IP	0.005	0.025	0.124	0.124	0.042

[†] $P < 0.1$, * $P < 0.05$, ** $P < 0.01$, *** $P < 0.001$.

EU = Ease of Use, U = Usefulness, V = Vulnerability, S = Severity, SN = Subjective Norm, A = Attitude, PBC = Perceived Behavioral Control, IP = Intention to protect.

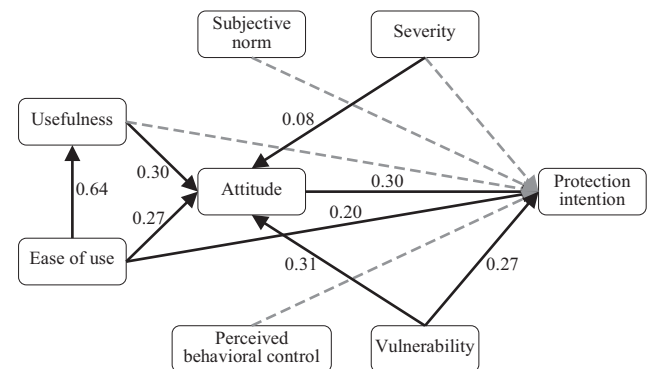


Fig. 1. Paths of factors affecting intention to protect personal information on Facebook.

information on Facebook had significant impacts on people’s positive attitudes about the protection of personal information on Facebook. Further, the intention to protect personal information on Facebook increased when it was perceived that protecting personal information on Facebook was not difficult.

Second, among the three variables constituting the TPB model, only attitude ($\beta = 0.30$, $t = 2.05$, $p < 0.05$) had a positive effect on the intention to protect personal information on Facebook. Subjective norm and perceived behavioral control did not significantly explain the dependent variable. This finding indicated that the higher the positive attitude toward personal information protection on Facebook, the higher the intention to protect personal information. In addition, it showed that the

behavior of personal information protection on Facebook is not influenced by perceptions of significant others or a person's will.

Third, both severity ($\beta = 0.08$, $t = 0.64$, $p < 0.01$) and vulnerability ($\beta = 0.31$, $t = 2.53$, $p < 0.05$) from PMT had positive effects on the attitude toward protecting personal information on Facebook. However, only vulnerability ($\beta = 0.27$, $t = 2.09$, $p < 0.05$) had a direct effect on that intention. Severity had an indirect effect on the intention to protect personal information on Facebook through attitude. These results indicated that as vulnerability and severity increase, demonstrating the severity of the threat to personal information infringement, the attitude toward personal information protection on Facebook becomes more positive. This finding suggested that the intention to protect personal information on Facebook can be induced by a concrete perception that a person could be exposed to personal information infringement.

Additionally, TAM- and PMT-related variables showed 29.2% of the explanatory power for the attitude toward personal information protection on Facebook. In addition, TAM, TPB, and PMT variables showed 36.4% of the explanation power for the intention to protect personal information on Facebook. Comparatively, TPB had 28.3% of the explanation power, TAM 9%, PMT 17.5%, the integrated model of PMT and TAM 24.1%, the integrated model of TAM and TPB 29%, and the integrated model of PMT and TPB 32.8% for the dependent variable.

V. Discussion and Conclusions

1. Theoretical Implications

This study generated several theoretical contributions to the study of the intention to protect personal information. We proposed a new model for predicting the intention to protect personal information on Facebook by integrating three models (TAM + TPB + PMT). The integrated model of TAM, TPB, and PMT showed a good model fit to predict technology-based behavior of personal information protection on Facebook.

In some recent studies, researchers attempted to increase the explanatory power for predicting technology-based behavioral intention by integrating TAM and TPB [15], [16]. Other studies have been conducted on different combinations of three models, integrating PMT with TAM or with TPB [13], [21], to improve the explanatory power for dependent variables (that is, protection intention). Based on these studies, this study integrated three theories and proposed a new approach that had never been attempted. The results showed that the integrated model of

TAM, TPB, and PMT significantly improved the explanatory power in predicting the intention to protect personal information on Facebook.

The results suggested that adding different variables to the integrated model to predict a particular type of behavior can heighten the explanatory power by removing weak points. For example, TAM focuses on usefulness and ease of use to explain behavioral intention related to a technology-based service. However, applying TAM may be unsuitable for smart and social media (for example, SNSs) because TAM only considers personal factors (that is, perceived usefulness and ease of use). Thus, it is necessary to add TPB to the model because TPB covers key aspects of human society and efficacy. Furthermore, a protective barrier against the leakage of personal information is based on rationality in human cognition. Hence, the study not only attempted to predict technology-based information protection behavior by employing an integrated model of three different theories, but also confirmed the model's usefulness for predicting the intention to protect personal information on Facebook.

Usefulness and ease of use from TAM had a positive effect on attitude. This result suggested that when one perceives personal information protection on Facebook to be useful and easy to do, the attitude toward protecting personal information on Facebook increases. Ease of use, but not usefulness, had a *direct* effect on the intention to protect personal information on Facebook. This result indicated that technological features enabling ease of use are more critical for users' privacy protection behavior.

We found that ease of use affected usefulness and that perceived usefulness also significantly influenced user behavioral intention toward personal information protection on Facebook through attitude. This indicated that perceived usefulness of personal information protection on Facebook had an indirect effect on the intention to protect personal information on Facebook.

Among TPB variables, only attitude had a positive effect on the intention to protect personal information on Facebook. That is, a more positive attitude toward personal information protection on Facebook leads to a higher level of privacy protection intention. Thus, improving people's attitudes toward information protection behavior on Facebook could help to prevent the leakage of personal information on Facebook. It is noticeable that social variables (that is, subjective norm and perceived behavioral control) did not provide a significant explanation for the intention to protect personal information.

One plausible explanation is that Korean Facebook users may perceive personal information protection

behavior as personal behavior and that they cannot control their information on Facebook. It suggested that the perception of the severity of personal information threats on Facebook was not higher than we thought. In other words, personal information protection behavior on Facebook was performed when a person prefers the protective behavior for personal reasons, and others' viewpoints or social influence or whether the protective behavior can actually be performed are unimportant.

The results also showed that severity and vulnerability contributed to the formation of a positive attitude toward personal information protection on Facebook. When the leakage of personal information from Facebook was perceived as serious, and vulnerability as a user perceived the likelihood of information leakage was high, a positive attitude toward protection increased. Vulnerability, but not severity, had a *direct* effect on the intention to protect personal information on Facebook, whereas severity did not have a direct effect on the intention to protect personal information. This result indicated that a user's protection intention depends not on the perception of severity but only on vulnerability to the leakage of personal information from Facebook.

2. Practical Implications

The study also had several practical implications. According to our findings, it is important to develop campaign activities to increase positive attitudes toward personal information protection behavior to motivate personal information protection behavior on Facebook. Using various media, public relations (PR) activities should be conducted to disseminate the perception that the leakage of Facebook and other online-based personal information can cause serious social and individual issues. Furthermore, it would be an effective campaign strategy to promote the idea that a person should take action to prevent the leakage of personal information with regard to setting personal information protection. Thus, the cooperation of the government, educational institutions, and a variety of mass media would be a very important role in such PR campaigns.

This finding indicated that TAM variables had significant impacts on attitude toward personal information protection on Facebook, but they did not directly induce personal information protection behavior. Thus, it is essential to increase awareness that setting personal information protection on Facebook should be convenient as well as easy in order to directly promote personal information protection behavior on Facebook. As a consequence, Facebook constantly provides information about setting

personal information protection, and also makes efforts to convey the message that the setting is easy.

Our findings showed that PMT variables had significant effects on improving positive attitudes toward personal information protection on Facebook, but only vulnerability induced personal information protection behavior. Therefore, it is necessary to focus on the perception that personal information is vulnerable to information leakage when personal information protection is not set on Facebook in order to directly induce personal information protection behavior on Facebook.

Recently, it has been seen that the leakage of personal information is spreading as a social problem [28], but people do not regard this issue seriously. This study showed that what is important for personal information protection behavior was not the severity of social phenomena, but the belief that they can bring a disadvantage or vulnerability. Therefore, there is a need for specific message strategies to induce personal information protection behavior, which focuses on how much harm the leakage of personal information could result in and how vulnerable a person can become from the leakage of personal information when he or she does not perform personal information protection behavior.

In addition, a sort of fear appeal could be effective as a message strategy to induce personal information protection behavior. Because severity had an indirect effect through attitude on the intention to protect personal information on Facebook, message strategies need to include some content emphasizing the severity of information leakage on Facebook and focusing on the system's vulnerability to such leakage.

3. Limitations and Future Research

Despite such contributions, this study has several limitations. First, this study utilized variables from only three theories to predict the intention to protect personal information on Facebook. However, there are various other independent variables that could explain the dependent variable (that is, protection intention). This study has the limitation that it did not maximize the explanatory power of the dependent variable by incorporating a large variety of independent variables into the model. Therefore, future research could incorporate related variables such as self-efficacy.

Second, from the perspective of TPB, a behavioral intention is highly relevant to the actual behavior, but is not identical. Using behavioral intention and not measuring actual behavior directly can be another limitation. Future research could examine actual behavior.

Another limitation is that our sample was drawn from a single country, South Korea. The homogeneity of the sample may limit the generalizability of the study. Further, future research could replicate this study across several cultures and countries.

In addition, this study did not examine differences between socioeconomic subgroups. Identifying differences between gender and age groups is needed. Future research could explore the effects of demographic characteristics on the intention to protect personal information on Facebook.

Finally, personal information protection behavior on Facebook can be diverse. The neglect of diverse behavior intention (for example, the level of personal information protective behavior intention) can be a limitation. Future research could consider different levels of information protection intentions to measure behavioral intention.

4. Conclusion

This study examined the predictors of intention to protect personal information on Facebook. The findings of this study showed that the effectiveness of setting protection on Facebook (that is, usefulness) and the ease of using the protection function (that is, ease of use) had significant effects on attitudes toward protection behavior. The results also revealed that risk factors (privacy risk severity and vulnerability) had significant effects on privacy protective behaviors on Facebook.

Acknowledgements

This work was supported by the research fund of Hanyang University (HY-2013-I).

References

- [1] D. Boyd and N. Ellison, "Social Network Sites: Definition, History and Scholarship," *J. Comput. Mediated. Commun.*, vol. 13, no. 1, Oct. 2007, pp. 210–230.
- [2] M. Thelwall, "Social Network Sites: Users and Uses," *Adv. Comput.*, vol. 76, 2009, pp. 19–73.
- [3] S. Livingstone, K. Olafsson, and E. Staksrud, *Social Networking, Age and Privacy*, LSE, London, EU Kids Online, 2011.
- [4] Y. Al-Saggaf and S. Nielsen, "Self-Disclosure on Facebook Among Female Users and its Relationship to Feelings of Loneliness," *Comput. Human Behavior*, vol. 36, July 2014, pp. 460–468.
- [5] F.D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly*, vol. 13, no. 3, Sept. 1989, pp. 318–339.
- [6] M. Fishbein and I. Ajzen, *Beliefs, Attitude, Intention and Behaviour: An Introduction to Theory and Research*, Reading, MA, USA: Addison-Wesley, 1975.
- [7] F.D. Davis, R.P. Bagozzi, and P.R. Warshaw, "User Acceptance of Computer Technology," *Manage. Sci.*, vol. 35, no. 8, Aug. 1989, pp. 982–1003.
- [8] J. Shah and E.T. Higgins, "Expectancy \times Value Effects: Regulatory Focus as Determinant of Magnitude and Direction," *J. Personality Soc. Psychol.*, vol. 73, no. 3, Sept. 1997, pp. 447–458.
- [9] N. Park, K.M. Lee, and P.H. Cheong, "University Instructors' Acceptance of Electronic Course Ware: An Application of the Technology Acceptance Model," *J. Comput. Mediated Commun.*, vol. 13, no. 1, Oct. 2007, pp. 163–186.
- [10] D. Gefen and D.W. Straub, "Gender Differences in the Perception and Use of E-Mail: An Extension to the Technology Acceptance Model," *MIS Quarterly*, vol. 21, no. 4, Dec. 1997, pp. 389–400.
- [11] G. Choi and H. Chung, "Applying the Technology Acceptance Model to Social Networking Sites (SNS): Impact of Subjective Norm and Social Capital on the Acceptance of SNS," *Int. J. Human Comput. Interaction*, vol. 29, no. 10, Jan. 2013, pp. 619–628.
- [12] I. Ajzen, "The Theory of Planned Behavior," *Organizational Behavior Human Decision Process.*, vol. 50, no. 2, Dec. 1991, pp. 179–211.
- [13] P. Ifinedo, "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Comput. Security*, vol. 31, no. 1, 2012, pp. 83–95.
- [14] B. Bulgurcu, H. Cavusoglu, and I. Banbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly*, vol. 34, no. 3, 2010, pp. 523–548.
- [15] Y. Lu, T. Zhou, and B. Wang, "Exploring Chinese Users' Acceptance of Instant Messaging Using the Theory of Planned Behavior, the Technology Acceptance Model, and the Flow Theory," *Comput. Human Behavior*, vol. 25, no. 1, Jan. 2009, pp. 29–39.
- [16] M.C. Lee, "Factors Influencing the Adoption of Internet Banking: An Integration of TAM and TPB with Perceived Risk and Perceived Benefit," *Electron. Commerce Res. Appl.*, vol. 8, no. 3, 2009, pp. 130–141.
- [17] R. Rogers, "Cognitive and Psychological Processes in Fear-Based Attitude Change: A Revised Theory of Protection Motivation. In *Social Psychophysiology: A Sourcebook*, New York, USA: Guilford Press, 1983, pp. 153–176.

- [18] C.L. Anderson and R. Agarwal, "Practicing Safe Computing: A Multi-Method Empirical Examination of Home Computer User Security Behavioral Intention," *MIS Quarterly*, vol. 34, no. 3, 2010, pp. 613–643.
- [19] K.H. Beck and A. Frankel, "The Effects of Health Threat Seriousness and Personal Efficacy Upon Intentions and Behavior," *J. Appl. Social Psychol.*, vol. 11, 1981, pp. 401–415.
- [20] Y.H. Lee, "Understanding Anti-Plagiarism Software Adaption: An Extended Protection Motivation Theory," *Decision Support Syst.*, vol. 50, no. 2, 2011, pp. 361–369.
- [21] Y.H. Lee and K.R. Larsen, "Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-Malware Software," *Eur. J. Inform. Syst.*, vol. 18, 2009, pp. 177–187.
- [22] N. Mohamed and J.H. Ahmad, "Information Privacy Concerns, Antecedents and Privacy Measure Use in Social Networking Sites: Evidence from Malaysia," *Comput. Human Behavior*, vol. 28, no. 6, 2012, pp. 2366–2375.
- [23] V. Venkatesh and F.D. Davis, "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies," *Manage. Sci.*, vol. 46, no. 2, 2000, pp. 186–204.
- [24] I. Ajzen, "Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior," *J. Appl. Soc. Psychol.*, vol. 32, 2002, pp. 665–683.
- [25] X. Wang and S.R. McClung, "Toward a Detailed Understanding of Illegal Digital Downloading Intentions: An Extended Theory of Planned Behavior Approach," *New Media Soc.*, vol. 13, no. 4, 2011, pp. 663–677.
- [26] M. Hajli, "An Integrated Model for E-Commerce Adoption at the Customer Level with the Impact of Social Commerce," *Int. J. Inform. Sci. Manage.*, Special Issue, 2012, pp. 77–97.
- [27] D. Gefen and D.W. Straub, "Consumer Trust in B2C E-Commerce and the Importance of Social Presence: Experiments in E-Products and E-Services," *Omega*, vol. 32, no. 6, 2004, pp. 407–424.
- [28] I.A. Junglas, N.A. Johnson, and C. Spitzmüller, "Personality Traits and Concern for Privacy: An Empirical Study in the Context of Location-Based Services," *Eur. J. Inform. Syst.*, vol. 17, no. 4, 2008, pp. 387–402.



Bum Soo Chon received his BS degree in journalism & communication, and his MA degree in journalism & communication, from Hanyang University, Rep. of Korea, in 1991 and 1993, respectively. He received his PhD degree in communication at the State University of New York at

Buffalo, USA, in 2002. Currently, he is a professor in the Department of Journalism and Communication, Hanyang University, Ansan, Rep. of Korea. His research interests are in digital media and content, and media industry and management.



Jeong-Ki Lee received his BS degree in mass communication from Tongmyoung University, Busan and his MA degree in mass communication and PhD degree in communication at Hanyang University, Rep. of Korea, in 2007, 2009, and 2013, respectively. He is a principal researcher in the Center for Teaching & Learning at Hanyang University. His research interests include media effects, media law, media education, and smart advertising.



HyeonJu Jeong received her BS degree in Journalism, MS degree in Public Relations from California State University, USA and PhD degree in Public Relations from Sungkyunkwan University, Seoul, Rep. of Korea, in 1994, 2004, and 2013, respectively. Currently, she is an assistant professor in the department of advertising and public relations, Catholic Kwandong University, Gangneung, Rep. of Korea. Her research interests include public relations, crisis management, and health communication.



Jowon Park received his BA and MA degrees in journalism and mass communication from Hanyang University, Seoul, Rep. of Korea, in 1989 and 1991, respectively. He received his another master's degree in Communication from Indiana State University, USA, in 1996. His PhD degree is in Communications from the University of Tennessee, Knoxville, USA. He was with the Korean Broadcasters Association from 1991 to 1994. From 2000 to 2012, he worked for the Korea Culture and Tourism Institute where he held the position of research director of Cultural Industry Policy Research Division. Since 2012, he has been a professor in the Department of Journalism and Mass Communication at Hanyang University ERICA Campus in Ansan, Rep. of Korea. His research interests include media consumption, art and cultural consumption, and media psychology.



Jonghwa Park received his BS degree in technology management from Ulsan National Institute of Science and Technology, Rep. of Korea in 2014. He is currently pursuing a PhD degree at the School of Management Engineering, Ulsan National Institute of Science and Technology. His main research interests are user adoption and sensemaking of new information technology including digital media, mobile technology services, and the Internet of Things.