The Educational Review, USA, 2019, 3(10), 152-163
http://www.hillpublisher.com/journals/er

A Study of Determinants of Teenagers' Privacy Protection Intentions on Social Networking Sites

Di Wang

C202, Macau University of Science and Technology, Avenida Wai Long, Taipa, Macau, China

How to cite this paper: Wang, D. (2019). A Study of Determinants of Teenagers' Privacy Protection Intentions on Social Networking Sites. *The Educational Review, USA,* 3(10), 152-163.

http://dx.doi.org/10.26855/er.2019.10.004

***Corresponding author:** Dr. Wang Di, Faculty of Humanities and Arts, Macau University of Science and Technology.

E-mail: dzwang@must.edu.mo

Abstract

Using protection motivation theory, this study aimed to understand factors that affect teenagers'privacy protection intention on a social network site, Wechat Moment. Perceived severity, perceived vulnerability, self-efficacy and response efficacy were predicted to be positively related to privacy protection intention, while perceived rewards and response costs were predicted to be negatively related to privacy protection intention.

Results from a survey of 608 Chinese teenagers showed that perceived severity, perceived vulnerability, self-efficacy and response efficacy were positively related to teenagers'privacy protection intention on Wechat Moment, while response costs and perceived rewards were not related to teenagers'privacy protection intention on Wechat Moment.

Keywords

protection motivation theory, privacy protection intention, social networking sites, Wechat Moment

1. Introduction

Social networking sites (SNSs for short), by design, are platforms to write about oneself (Wang, 2017). Sundén (2003) argued that, in order to exist online, individuals must first write themselves into being. Refaining from writing any personal information on SNSsis quite challenging, especially for teenagers. In comparison to other age groups, teenagers are found to be more active in sharing information on SNSsthan the general population (China Internet Network Information Center, 2016). Many teenagers upload detailed information about their lives on SNSs, including details about dining, partying, and even some intimate behaviors. Such behaviors might bring about negative consequences, such as rejection from universities (Trimble, 2017), and sex video leakage (Jiang, Dong & Watson, 2015), etc. Accordingly, it is crucial to study what factors could increase teenagers' privacy protection intention.

Scholars believe that people hold two opposing motives in using SNSs: privacy concerns and impression management (Utz& Kramer, 2009).As a result, privacy is a compromise between pressures for withdrawal and disclosure (Tufekci, 2008).Setting restrictive privacy settings on SNSs can fulfill both needs—the need to protect one's privacy from unwanted "friends", and the need to convey personal information so as to manage the impression given to desired friends on SNSs. Teenagers can block their parents, other relatives, teachers, strangers, and any other people to whom they do not want their information to be disclosed. However, many teenagers still hold public SNS accounts (Pew Research Center, 2013). To understand this, this study adopts protection motivation theory to examine the determinants of teenagers' privacy protection intention on SNSs.

Specifically, we want to explore whether teenagers feel that they are vulnerable to privacy leakage on SNSs; whether they feel such privacy leakage will bring serious negative consequences to themselves; whether they are technically able to adjust their privacy settings on SNSs; whether they feel setting privacy settings on SNSs will be useful for protecting their privacy; whether they think setting privacy settings takes too much time or energy; and whether choosing not to use privacy settings would bring benefits to themselves. We further want to test whether these six factors may predict

teenagers' privacy protection intention on SNSs in the case of one of the most popular Chinese SNSs, Wechat Moment (WeChat Chatterbox, 2016).

Previous research have applied protection motivation theory to explain the determinants of Korean young adolescents' online privacy concernsand coping behavior (Youn, 2009), and the determinants of American student's behavioral intention to share information on social media (Banks, Onita, &Meservy, 2010). However, none of them have applied the all the theoretical predictors of protection motivation in one study. Thus, this study shall fill in the knowledge gap by applying all six predictors of protection motivation theory in one study and test whether all six predictors would predict privacy protection behavioral intention. Another motivation of the current study is to inform Chinese media practitioners and educators the determinants of teenagers' protection behavior so that they could apply them in their media practice and educational practice.

2. Literature Review

2.1. Online privacy protection behaviors

There are many definitions of privacy. One of the most-cited definitions of privacy is "the right to prevent the disclosure of personal information to others" (Westin, 1967, p. 7).Lwin, Wirtzand Williams(2007) found that there are generally three ways for people to protect their online privacy— fabrication, protection, and suppression. Fabrication refers to providing false or incomplete personal information in order to hide one's true identity. Protection refers to setting password protection, setting access permissions, reading the website privacy agreement, and conductingother technical procedures to proactively protect privacy. Suppression means that the Internet user refuses to provide any personal information or immediately terminates the online activity so as to protect privacy.Lwin, Wirtzand Williams (2007) argued that, compared to protection, fabrication and suppression are negative ways to protect online privacy, which may cause negative impacts on online development. Thus, in this study we shall focus on protection-based online privacy behavior. The privacy protection behavior under study is the willingness ofteenagersto userestrictive privacy settings to protect their privacy on Wechat Moment. We shall use protection motivation theory as a framework to explore predictors of this privacy protection behavioral intention.

2.2. Protection motivation theory and privacy protection on SNSs

Protection motivation theory (Rogers, 1975, 1983) proposes that two appraisals, threat appraisal and coping appraisal, predict the intention toprotect oneself from a threatened event, which further predicts protective behavior (Milne, Sheeran&Orbell, 2000).Specifically, threat appraisalis composed of perceived severity,perceived vulnerability, and perceived rewardsassociated with a riskybehavior. Coping appraisal includes self-efficacy, response efficacy, and response costs. Next, we shall review the six elements of protection motivation theory and their relationships with protection behaviors on SNSs.

2.3. Perceived vulnerability

Perceived vulnerability is defined as the assessment of the probability of exposure to the threat (Lee, 2011). On SNSs, sharing personal information has become a popular activity. SNSs users are thus vulnerable to information leakage, which could lead to negative consequences such as identity theft, tracking, harassment, and extortion (Lipford, Besmer& Watson, 2008).

Perceived vulnerability has been found to be negatively related to personal information revelation on SNSs (Youn, 2005) and positively related to privacy protection behaviors such as seeking help from parents and teachers and refraining from using risky websites (Youn, 2009).Dinev and Hart (2004) also found that there is a positive correlation between the perceived risk of privacy exposure and the willingness to protect privacy.

Not all studies in the literature found similar results. Zhang and Mcdowell (2009) found that there was no significant relationship between users' perceived vulnerability to information security and their willingness to use strong passwords. The authors explained that their results do not mean that perceived vulnerability is not an important predictor of adopting preventive behaviors; rather they could be due to the respondents' havingperceived rather low levels of severity and vulnerability in relation to password breaches. As there are still mixed results in the literature, we shall resolve the discrepancy by testing the effect of perceived vulnerability on privacy protection intention in the current study.

In this study, we define perceived vulnerability as teenagers' feeling that they are vulnerable to the threat of information leakage on SNSs. For instance, teenagers may feel that disclosing personal information on SNSs could lead to identity theft, disclosing cellphone number on SNSs may result inspam messages, etc. Once teenagers feel that they are vulnerable to personal information disclosure, they will carry out privacy protection behaviors in order to reduce the potential threat.Therefore we hypothesize:

H1: Perceived vulnerability to privacy risks resulting from information disclosure is positively related to teenagers' privacy control intention on SNSs.

2.4. Perceived severity

Perceived severity is defined as the perceived severity of the consequences of a threat (Ifinedo, 2012). When a person perceives a threat, he/she tends to adjust their behaviors based on the anticipated severity of the outcome, thereby reducing risk. The more serious theconsequences a person perceives that his/her bad behavior will result in, the stronger the willingness to take the recommended behavior (Lee, 2011).

Yoon (2012)'s study found thatthe perceived severity of privacy disclosure riskis positively related to the willingness of individuals to take action to protect privacy.Perceived severity has also been found to be negatively related to the behavioral intention of an individual to reveal personal information on SNSs (Banks, Onita, &Meservy, 2010).

In this study, we define the perceived severity of privacy risk as teenagers' perception that their SNSs sharing behavior willexpose them to some degree of harm. The more serious teenagers perceive the threat of privacy disclosure to be, the stronger the actions they will take toprotect their privacy, thereby reducing the negative consequences of privacy leakage. Therefore, we hypothesize:

H2: Perceived severity of privacy risks resulting from information disclosure is positively related to teenagers' privacy control intention on SNSs.

2.5. Self-efficacy

Self-efficacy refers to the extent to which individuals feel they are able to perform the recommended behavior(Ifinedo, 2012).Studies found that people have different technical skills in the context ofprivacy settings. For instance, Brandtzæg, Lüders, and Skjetne (2010) found that, compared to younger adults, those who were over 40 years old had more difficulties in understanding the navigation logic and privacy settings of Facebook.

Workman (2008) found that self-efficacy positively affects the user's willingness to use information systems. Yoon (2012)'s study showed that the higher the self-efficacy of students, the more they are willing to implement information security procedures.

On the other hand, some research found self-efficacy to be unrelated to privacy concern and privacy protection behavior. Youn (2009) found that privacy self-efficacy was not significantly related to privacy concerns for teenagers. Dienlin and Metzger (2016) found privacy self-efficacy was not significantly related to Facebook self-disclosure.

These discrepant findings can be explained. We argue that privacy self-efficacy is positively related to use of privacy settings, rather than privacy concern or self-disclosure. If teenagers are confident that they are able to use privacy settings to protect their privacy, they are more likely to do so. At the same time, if teenagers have the knowledge and skills to use privacy settings, they may still have other privacy concerns due to other concerns, such as believingthat privacy settings will be ineffective in protecting their privacy. Teenagers may even disclose more due to having set restrictive privacy settings. Thus, we make the following hypothesis:

H3: Privacy self-efficacy is positively related to teenagers' privacy control intention on SNSs.

2.6. Response efficacy

Response efficacy refers to an individual's beliefs about whether the recommended behavior will be effective in reducing or eliminating thenegative consequences (Zhang & McDowell, 2009).

In a study of whether students are willing to implement network information security behavior, Yoon (2012) found that response efficacy and the implementation of information security behavior have a positive correlation.Response efficacy was also found to be positively related to behavioral intention associated with using virus protection software

(Lee, Larose &Rifon, 2008). Moriarty (2009)'s study showed that publishing clinical trial reports regularly can increase women's response efficacy, motivatingthem to perform aerobic exercise.

Whether response efficacy is negatively related to privacy protection behaviors on SNSs has not been studied in the literature, and thus remains to be tested in the current study. In this study, we define response efficacy as teenagers' degree of belief that using privacy settings will be effective in protecting their privacy on SNSs. The more teenagers believe that the protection behavior is effective, the more they will be inclined to conduct this privacy protection behavior. Therefore, we make the following hypothesis:

H4: Response efficacy is positively related to teenagers' privacy control intention on SNSs.

2.7. Response costs

Response costsare defined as the perceived cost to individuals of adopting the recommended behavior (e.g. in terms of time, money, energy, obstacles, and embarrassment) (Zhang & McDowell, 2009). Response costs will hinder adoption of the recommended behavior. If individuals perceive that they will pay a lot in order to adopt the recommended behavior, their willingness to do so will be reduced. They will usually hesitate and reconsider whether such recommended behavior is necessary (Peace, 2003).Conversely, if it costs little to adopt the recommended behavior, people are usually more willing to adopt that behavior (Peachmann, 2008).

In the literature, response costs have not been studied as a predictor of privacy protection behavior on SNSs. The time and effort one requires to learn about the privacy settings, as well as thetime and effort one requires to use the privacy settings every time one posts a message,could reduce the likelihood of privacy protection behavior.Thus, we make the following hypothesis:

H5: Response costs arenegatively related to teenagers' privacy control intention on SNSs.

2.8. Perceived rewards

Rewards can come from both internal factors and external factors. An intrinsic reward is an intangible reward that could come from a sense of achievement, or recognition, or a conscious satisfaction while an extrinsic reward is a tangible reward that is given to someone for accomplishing something, such as candy, prizes, money, positive evaluation, and praise (Deci, 1971).Deci, Koestner and Ryan (1999)'s meta-analysis show that both intrinsic and extrinsic rewards can usually induce an individual to conduct the corresponding behavior.

Christofides, Muise, and Desmarais (2009)'s study found that the need for popularity predicts personal information disclosure among adolescents. Dienlin and Metzger (2016)'s study found respondents who reported that they would get more social benefits on Facebook also posted more personal information.

In this study, we define rewards as receiving attention, comments and "likes" from posting on Wechat Moment. To a certain extent, using restrictive privacy settings can be an impediment to obtaining these rewards. Therefore, we hypothesize:

H6: Perceived rewards of not setting restrictive privacy settings are negatively related to privacy control intention on SNSs.

3. Method

The main purpose of this study is to explore the effects of perceived vulnerability, perceived severity, response costs, response efficacy, self-efficacy, and perceived rewards on teenagers' privacy protection behavioral intention on Wechat Moment. We conducted a paper and pencilquestionnaire that asked the above variables as well as the information about teenagers' SNS use and demographic variables. All the main dependent and independent variables were asked with scales that were adapted from previous studies except rewards.Perceived vulnerability scale and perceived severity scale was adapted from Bank, Onita andMeservy(2010)'s scale. Response costs, response efficacy, and self-efficacy scale were adapted from the scale of Ifinedo (2012) and the scale of Johnston (2010). In addition, demographic variables and Wechat usage information were asked to provide background information for the study.

3.1. Participants

Participants were Chinese teenage students from a junior high school and a senior high school in southern part of

China. One thousand participants from the two schools were asked to fill in a paper and pencilquestionnaire.Participants who have not used Wechat Moment were excluded from the sample. After eliminating incomplete responses and ineligibleparticipants through data filtering, 608 valid responses were selected as the sample. Of theseparticipants, 52.8% were malesand 47.2 % were females.Participants ranged in age from 11to 19 years old (M = 15.39, SD = 1.79). They have used the Internet for 4.30 years on average (SD = 1.14) and have used Wechat Moment for 1.81 years on average (SD = .99).

3.2. Measures

Privacy control intention. The SNS under study, Wechat Moment, has the function of blocking people from accessing one's Wechat Moment. People can block a "friend" from viewing theirWechat Moment completely. In addition, each time individuals post on Wechat Moment, they have four options: (a) public (everyone can view it), (b) private (can only be viewed by oneself), (c) can only be viewed by those who are selected, and (d) cannot be viewed by those who are selected. This option allows users to block certain people from seeing certain posts that they do not want them to see.

Privacy control intention was measured by five items "(1) In the future, I will set up accesspermissionsfor some people", "(2) In the future, I will set access permissions when posting on Wechat Moment more often", "In the future, I will set access permissionswhen posting information about (3) my family/ (4) my friends/ (5) myself." Items were all rated with a 5-point Likert scale from 1 = "strongly disagree" to 5 = "strongly agree."Cronbach's alpha reliability estimate was high at 0.86.

Perceived vulnerability. Perceived vulnerability was measured by six items "Disclosing personal information on Wechat Moment may lead to (1) abuse of my personal information/ (2) identity lost/ (3) economic losses/ (4) interference of my life/ (5) receiving spam messages/ (6) receiving spam emails." Items were all rated with a 5-point Likert scale from 1 = "strongly disagree" to 5 = "strongly agree."

Perceived severity. Perceived severity to privacy risks was measured by six items "Revealing (1)my phone number/ (2) my email address/ (3)photos of myself/ (4) photos of my family/ (5) photos of my friends/ (6) my location on Wechat Moment will result in significant losses to me." Items were all rated with a 5-point Likert scale from 1 = "strongly disagree" to 5 = "strongly agree."

Self-efficacy. Privacy self-efficacy was measured by three items "(1) I can useprivacy settings of Wechat Moment by myself. / (2) It is easy for meto useprivacy settings of Wechat Moment./ (3) I have the ability to solve the problems with using privacy settings on Wechat Moment" Items were all rated with a 5-point Likert scale from 1 = "strongly disagree" to 5 = "strongly agree."

Response efficacy. Perceived response efficacy was measured by six items "Setting privacy settings can (1) protect personal information/ (2) protect friends' information/ (3) protect family's information/ (4) reduce unnecessary misunderstandings/ (5) reduce the interference of others/ (6) reduce parents' worries." Items were all rated with a 5-point Likert scale from 1 = "strongly disagree" to 5 = "strongly agree."

Response costs. Response costs were measured by three items "It takes a lot of (1) time/ (2) effort to set privacy settings. (3) If someone knows that I have blocked him/her, it will offend that person. "Items were all rated with a 5-point Likert scale from 1 = "strongly disagree" to 5 = "strongly agree."

Perceived rewards. Perceived rewards of not conducting privacy protection behavior were measured by four items "Do not set access permissions can (1) show more people the information I post on Wechat Moment/ (2)make more people follow me."Items were both rated with a 5-point Likert scale from 1 = "strongly disagree" to 5 = "strongly agree."

Internet experience. Internet experience was measured by a question "How long have you been using the Internet?" Responses were coded as "less than 1 year = 1, 1-2 years (including one year) = 1.5; 2-3 years (including two years) = 2.5; 3-4 years (including three years) = 3.5; 4-5 years (including four years) = 4.5; more than 5 years and above = 5."

Wechat Moment experience. Wechat Moment experience was measured by a question "How long have you been using the Wechat Moment?" Responses were coded as "less than half a year = .5, six months to one year = .75, 1-2 years (including one year) = 1.5; 2-3 years (including two years) = 2.5; 3-4 years (including three years) = 3.5; 4-5 years (including four years) = 4.5; more than 5 years and above = 5."

Wechat Moment posting frequency. Wechat Moment posting frequency was measured by a question "How often do you post on Wechat Moment on average?" Responses were coded as times per day, "never = 0, once every month = .033,

several times a month = .067, once every week = .142, several times a week = .5, once a day = 1, 2-3 times a day = 2.5; 4 times a day or more = 4."

Posting privacy content. Respondents were asked which of the following information they posted on Wechat Moment most often—pictures or videos about oneself; pictures or videos about family or friends; original textual information about one's own life; original information that has nothing to do with oneself; forwarded information; The first three options were coded as posting privacy content (1), whilelatter two options were coded as posting non-privacy related information (0).

Disclosing personal information frequency. Disclosing personal information frequency was measured by asking participantshow often they disclose the following information "personal photos/videos, friends' photos/videos, family's photos/videos, home addresses, and real-time positioning." Items were all rated with a 5-point Likert scale from 1 = "never" to 5 = "always."

Blocked subjects. Blocked subjects was measured by asking participants the following question "Which of the following people do you have blockage to a certain extent? Parents, other relatives, teachers, familiar real life friends, not so familiar real life acquaintances, Internet friends who you havenot met in person." Responses were coded as 1 (do not let him/her see my Wechat Moment sometimes or completely), and 0 (do not block him/her), missing (he/she does not have a Wechat Moment account and non-applicable (do not have such relationships)).

Demographics. Respondents were asked about their gender (female =1, male = 0) and age (years).

4. Results

4.1. Descriptive Statistics

Results showed that about 61.02% teenagers posted personal information (photos or videos about oneself, friends, and family) more often than other contents on SNSs.They posted friends' pictures and videos most often (M = 1.74, SD = .93), followed by personal pictures and videos (M = 1.65, SD = .91), pictures about family (M = 1.47, SD = .76), real-time positioning (M = 1.38, SD = .71), and home addresses (M = 1.12, SD = .49).

Among these participants, 55.1% of the teenagers have blocked others before, 34.5% of the teenagers have never blocked anyone, 10.4% of the teenagers do not know how to block other people on Wechat Moment. The people blocked most often are relatives other than parents (43.6%), parents (42.2%), teachers (39.5%), Internet friends who one has not met in person (37.8%), not so familiar real life acquaintances (36.8%). The least blocked people are familiar friends in real life as only 8.5% of the teenagers have blocked them.

The means, standard deviations and the inter-correlations of the six predictor variables and dependent variables were presented in Table 1. The six predictor variableswere moderately correlated, indicating an acceptable degree ofmulticollinearity among predictors.

4.2. Reliability and Validity Check

Reliability and construct validity were first checked before using them for further analysis. Three types of reliability indices examined in this study were Cronbach's alpha, composite reliability, and average variance extracted. Acceptable levels of Cronbach's alpha, composite reliability, and average variance extracted were recommended as 0.70, 0.70, and 0.50 or higher, respectively (Bagozzi& Yi, 1988; Bearden; Netemeyer, & Mobley, 1993; Fornell&Larcker 1981). As shown in Table 2, the reliability of the scale measures (i.e., Cronbach's alpha > 0.73, composite reliability > 0.77, and average variance extracted > 0.55) exceeds the recommended values. Therefore, reliability was achieved.

Construct validity refers to how well item measures correlate with a theoretical construct. Two aspects of construct validity were examined in this study: convergent validity and discriminant validity. Convergent validity is established when each of the measurement items loads with a significant t-value on its latent construct (Gefen& Straub, 2005). Fornell and Larcker (1981) suggested that two criteria should be met in order to establish convergent validity: (a) all of the factor loadings should be significant and exceed 0.70 and (b) Average Variance Extracted (AVE) should be greater than 0.50. As can be seen in Table 3, all of the factor loadings were significant and exceed 0.70. Table 2 showed that all the AVEs were above 0.50. Thus, convergent validity was established.

Table 2. Cronbach's alpha, composite reliability, AVE and correlations.

Variables	α	CR	AVE	1	2	3	4	5
1. Response cost	0.73	0.77	0.55	0.74				
2. Severity	0.91	0.9	0.61	-0.18	0.78			
3. Vulnerability	0.91	0.9	0.61	-0.26	0.5	0.78		
4. Self-efficacy	0.79	0.79	0.56	-0.28	0.1	0.16	0.75	
5. Response efficacy	0.92	0.92	0.66	-0.27	0.36	0.46	0.35	0.81
6. Rewards	0.83	0.85	0.67	0.4	-0.28	-0.27	-0.11	-0.27

Note: CR stands for composite reliability, AVE stands for average variance extracted.

Discriminant validity exists when the item measures load highly on the theoretical construct and not highly on other factors (Gefen& Straub, 2005). To establish discriminant validity, Gefen and Straub (2005) suggest that the square root of the Average Variance Extracted (AVE) for each construct should be much larger than the correlation of the specific construct with any of the other constructs in the model and should be at least 0.50. Table 2 presents the correlations among constructs, with the square root of the AVE on the diagonal. The data showed that the shared variance (correlation) between each pair of constructs was lower than the average variances extracted (diagonal values). Thus, discriminant validity was established as well.

Table 3. Principal component analysis with varimax rotation.

Component	1	2	3	4	5	6
Vulnerability1	.18	.78	.16	-.04	.01	-.13
Vulnerability2	.17	.81	.18	-.03	.00	-.10
Vulnerability3	.14	.80	.22	-.05	.06	-.05
Vulnerability4	.16	.76	.24	-.06	.05	-.04
Vulnerability5	.18	.78	.19	-.15	.05	-.05
Vulnerability6	.18	.79	.18	-.11	.03	-.03
Severity1	.11	.28	.71	-.11	.03	-.02
Severity 2	.01	.27	.76	-.06	.04	-.04
Severity 3	.15	.12	.86	-.06	.00	-.06
Severity 4	.16	.17	.84	-.07	.01	-.08

Table 3. ***cont.***

Component	1	2	3	4	5	6
Severity 5	.10	.14	.83	-.07	.03	-.08
Severity 6	.16	.20	.72	-.13	-.01	-.03
Rewards1	-.21	-.08	-.16	.71	-.10	.08
Rewards 2	-.11	-.13	-.12	.88	.00	.19
Rewards 3	-.05	-.10	-.10	.89	.00	.17
Self-efficacy1	.23	.08	.00	-.05	.80	-.04
Self-efficacy2	.19	.02	.00	-.04	.83	-.13
Self-efficacy3	.04	.03	.06	.00	.82	-.11
Response efficacy1	.83	.20	.12	-.09	.08	-.11
Response efficacy2	.85	.15	.16	-.06	.07	-.06
Response efficacy3	.87	.20	.12	-.09	.07	-.08
Response efficacy4	.77	.16	.14	-.10	.13	-.07
Response efficacy5	.81	.16	.14	-.07	.11	-.10
Response efficacy6	.71	.15	.11	-.07	.14	-.06
Response costs1	-.07	-.12	.01	.17	-.10	.85
Response costs2	-.11	-.10	-.03	.13	-.07	.88
Response costs3	-.17	-.08	-.21	.12	-.13	.56

4.3. Test of Hypotheses

To test the hypotheses, ahierarchical regression was conducted by entering demographicvariables in the first step (age and gender), online usage information in the second step (Internet experience andWechat moment experience),perceive dvulnerability, perceived severity, self-efficacy, response efficacy, response costs, and perceivedrewards in the last step with privacy control intention as dependent variable.

As can be seen in Table 4, results showed that perceivedvulnerability was positively associated with teenagers' privacy control intention, $\beta = .11$, $p < .01$; perceivedseverity waspositively associated with teenagers' privacy control intention, $\beta = .16$, $p < .001$; self-efficacy was positively associated with teenagers' privacy control intention, $\beta = .19$, $p < .001$; response efficacy was positively associated with teenagers' privacy control intention, $\beta = .27$, $p < .001$; response costswere not significantly related to teenagers' privacy control intention, $\beta = -.06$, $p > .05$; perceivedrewards werenot significantly related with teenagers' privacy control intention, $\beta = -.06$, $p > .05$. Thus, H1, H2, H3, and H4 were supported. H5 and H6 were not supported.The VIF values of all the independent variables were less than 3, which showed that there was no multicollinearity among independent variables.

Age was found to be significantly negatively related to teenagers' privacy control intention, $\beta = -.09$, $p < .05$. R^2 showed that the six independent variables and one control variable explained 34.2% of the variance of privacy control intention.

Table 4. Linear regression analyses for perceived vulnerability, perceived severity, response costs, response efficacy, self-efficacy, and perceived rewards predicting on privacy control intention.

Predictor	β
Perceived vulnerability	.11**
Perceivedseverity	.16***
Self-efficacy	.19***
Response efficacy	.27***
Response costs	-.06
Perceivedrewards	-.06
Age	-.09**
R^2	.342
N	608

* $p < .05$, ** $p < .01$, *** $p < .001$.

5. Discussion

This study explored the factors predicting teenagers' privacy control intention on SNSs, using protection motivation theory. Results showed that perceived vulnerability, perceived severity, self-efficacy, and response efficacy positively predicts teenagers' privacy control intention while response costs and perceived rewards were not significantly related to teenagers' privacy control intention.

In terms of threat appraisal, two findings were consistent with our hypotheses while one was not. Consistent with our hypotheses, perceived vulnerability and perceivedseverity werefound to be positively related to privacy control intention. The teenagers in this study felt moderately vulnerable to privacy leakage on SNSs ($M = 3.84$, $SD = .77$). They also felt the consequences of privacy leakage on SNSs are moderately serious ($M = 3.45$, $SD = .85$).Educators could increase teenagers' privacy awareness on SNSs byshowing teenagers news coverage of the negative consequences of privacy leakage. They could also show teenagers how vulnerable they are to such privacy leakage by letting teenagers do experiments to test how easy it is to find out privacy about each other through their SNS accounts.

Contrary to our hypothesis, rewards were found to be not a significant predictor of privacy control intention. Perhaps, people consider setting restrictive privacy settings may not undermine the rewards they get on SNSs. After blocking unwanted friends, they could still get the approval and comments from their wanted friends. Therefore, rewards were not directly related to privacy control intention on SNSs.

In terms of coping appraisal, two findings were consistent with our hypotheses while one was not. Consistent with our hypotheses, self-efficacy and response efficacy were positively related to teenagers' privacy control intention. Teenagers in this study reported a moderately high self-efficacy ($M = 3.82$, $SD = .75$) and a moderately high response efficacy ($M = 3.81$, $SD = .73$), but there is still room for improvement. Educators could increase teenagers' media literacy by teaching teenagers the ways to protect their privacy on SNSs, such as setting privacy settings and inform them that such settings could effectively protect their privacy.

Contrary to our expectations, response costs were not found to be unrelated to privacy control intention. This could be due to that teenagersin our sample did not considersetting privacy settings to be very costly ($M = 2.40$, $SD = .68$). They did not think it will cost a lot of time and effort to set privacy settings, neither did they consider that it will upset people. As response costs are lowly rated, it is possible thatteenagers may not even consider response costs as a factor that could impact their adoption of privacy protection behavior. As a result, response costsmay be irrelevant to teenagers' privacy protection decision.

In addition to the independent variables, the study also found that age was negatively related to teenagers' privacy

control intention. That is, the younger the teenager, the more likely they are willing to use privacy control on their SNSs. Floyd (2000) found that for adults, there is no significant relationship between age and protective behavior; but for minors, the relationship between age and protection behavior become significant. Yoon (2012) believes that early adolescence should be considered as the best time to provide privacy education. They should be informed of the risks of using the Internet, and how to correctly protect their personal information. Consistent with previous studies, the findings from the current study also inform us that privacy education should be as young as possible.

One contribution of this study is that we applied protection motivation theory to explain the teenagers' privacy paradox on SNSs, that is, on the one hand, teenagers feel concerned about their privacy on SNSs, while on the other hand, a number of teenagers still hold a public SNS account without setting restrictive privacy control settings. Results from this study could explain the paradox. Although teenagers may feel they are vulnerable to privacy leakage on SNSs and that such leakage could lead to serious consequences, they may still hold a public SNS account due to low self-efficacy or low response efficacy.

Another contribution of the current study is the practical implications of the study's findings. This study comprehensively examined various predictors of teenagers privacy control intention. It is hoped that such findings could inform educators and media practitioners to guide teenagers to use SNSs safely and wisely. Educators could take advantage of the findings in the study to develop effective media literacy programs, which could encourage adolescents to develop safe Internet use habits.

Several limitations should be noted before we make further conclusion. First, the survey was conducted with a paper and pencil questionnaire. Of the 1000 questionnaires distributed, 283 respondents answered only part of the questions. Although they were informed that all the multiple choices were single answer questions, some respondents chose more than one answer for some questions. Future research could address this problem by using online questionnaire. The current study was done in a junior high school and a senior high school. The schools do not allow electronic devices such as cellphones to be used at school. Thus we could not use online questionnaire for the current study.

Second, 9th graders and 12th graders are comparatively less than the other graders in our sample because they are busy preparing the entrance exams to senior high school or university. The school officials did not want them to be disturbed and therefore the sample was not evenly distributed in terms of age. Further research could use a more balanced sample in terms of age.

Third, all the survey questions were based on self-report, which may suffer from memory error. Future research could let teenagers answer the questions at home, where they have access to their cellphones. They could check their actual SNS privacy settings, rather than based on recall.

Fourth, this study only studied setting restrictive privacy settings as a way of privacy protection. Other types of privacy protection, such as providing false information (fabrication), or refusing to provide any personal information (suppression) could be studied so as to understand the protection behavior more comprehensively.

To sum up, the results of this study provide support for the theorized linkage between threat appraisal, coping appraisal, on the one hand, and privacy protection behaviors, on the other. The study also extended our understanding of teenagers' SNS privacy protection behaviors. Educators could use the framework of the current study to develop media literacy programs that could teach teenagers to be safe and wise Internet surfers.

References

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, 16, 74-94.

Banks, M. S., Onita, C. G. & Meservy, T. O. (2010). Risky Behavior in Online Social Media: Protection Motivation and Social Influence. *Proceedings of the Sixteenth Americas Conference on Information Systems*, Lima, Peru, August, 12-15, 2010.

Bearden, W .O., Netemeyer, R. G., & Mobley, M. F. (1993). *Handbook of Marketing Scales: Multi-Item Measures for Marketing and Consumer Behavior Research*, Newbury Park, CA: Sage Publications.

Brandtzæg, P. B., Lüders, M., & Skjetne, J. H. (2010). Too Many Facebook "Friends"? Content Sharing and Sociability Versus the Need for Privacy in Social Network Sites. *International Journal of Human-Computer Interaction*, 26, 1006-1030.

China Internet Network Information Center (2016). 2015 Chinese Youth Internet Behavior Research Report. Retrieved Nov. 2, 2017 from http://www.cnnic.cn/hlwfzyj/hlwxzbg/qsnbg/201608/P020160812393489128332.pdf

Christofides, E., Muise, A. & Desmarais, S. (2009). Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? *Cyberpsychology& Behavior*, 12, 341-345, doi: 10.1089/cpb.2008.0226.

Deci, E. L. (1971). Effects of externally mediated rewards on intrinsicmotivation. *Journal of Personality and Social Psychology*, 18, 105-115.

Deci, E. L., Koestner, R., & Ryan, R. M. (1999). A meta-analytic review ofexperiments examining the effects of extrinsic rewards on intrinsic motivation. *Psychological Bulletin*, 125 (6), 627-668.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour& Information Technology*, 23(6), 413-422.

Dienlin, T. & Metzger, M. J. (2016). An Extended Privacy Calculus Model for SNSs: Analyzing Self-Disclosure and Self-Withdrawal in a Representative U.S. Sample. *Journal of Computer-Mediated Communication*, 21, 368-383.

Fornell, C., &Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, 18, 39-50.

Floyd, D. L., Prentice‐Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, 30(2), 407-429.

Gefen, D., & Straub, D. (2005). A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example. *Communications of the AIS*, 16, 91-109.

Ifinedo, P. (2012). Understanding information systems security policy compliance:An integration of the theory of planned behavior and the protection motivationtheory. *Computers & Security*, 31(1), 83-95.

Jiang, S., Dong, S. & Watson, I. (2015). China: Clothes come off in viral Uniqlo sex video. Retrieved Nov. 2, 2017 from http://edition.cnn.com/2015/07/15/asia/china-beijing-uniqlo-sex-video/index.html

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, 34 (3), 549-566.

Milne, S., Sheeran, P. & Orbell, S. (2000). Prediction and intervention in health-related behavior: a meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, 30, 106-143.

Moriarty, C. M. (2009). *Effects of self-efficacy and response efficacy messages in health news: Changing health attitudes and behavioral intentions*(Doctoral dissertation). University of Illinois at Urbana-Champaign, Urbana, Illinois

Lee, D., Larose, R., &Rifon, N. (2008). Keeping our network safe: a model of online protection behavior. *Behaviour& Information Technology*, 7, 445-454.

Lee, Y. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems*, 50(2), 361-369.

Lipford, H. R., Besmer, A., & Watson, J. (2008). Understanding Privacy Settings in Facebook with an Audience View. In *Proceedings of the USENIX Workshop on Usability, Psychology, and Security (UPSEC 2008)*, San Francisco, CA, USA.

Lwin, M. O., Stanaland, A. J., & Miyazaki, A. D. (2008). Protecting children's privacy online: How parental mediation strategies affect website safeguard effectiveness. *Journal of Retailing*, 84(2), 205-217.

Peace, A. G., Galletta, D. F., & Thong, J. Y. (2003). Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems*, 20(1),153-177.

Pechmann, C., Zhao, G., Goldberg, M. E., & Reibling, E. T. (2003). What to convey in antismoking advertisements for adolescents: The use of protection motivation theory to identify effective message themes. *Journal of Marketing*, 67(2), 1-18.

Pew Research Center. (2013). *Teens, Social Media, and Privacy*. Retrieved Nov. 2, 2017 from http://www.pewinternet.org/files/2013/05/PIP_TeensSocialMediaandPrivacy_PDF.pdf

Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91, 93-

114. doi:10.1080/00223980.1975.9915803.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In B. L. Cacioppo& L. L Petty (Eds.), *Social Psychophysiology: A Sourcebook* (pp. 153- 176). London, UK: Guilford.

Zhang, L., & McDowell, W. C. (2009). Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce*, 8(3-4), 180-197.

Sundén, J. (2003). *Material Virtualities: Approaching Online Textual Embodiment*. New York: Peter Lang.

Trimble, M. (2017). *Harvard Pulls Admission Offers After Explicit Posts*. Retrieved Nov. 2, 2017 from https://www.usnews.com/news/national-news/articles/2017-06-05/harvard-pulls-student-admission-offers-after-explicit-facebook-posts

Tufekci, Z. (2008). Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society*, 28, 20-36, doi: 10.1177/0270467607311484.

Utz, S., & Kramer, N. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 3(2). Retrieved Nov. 3 from https://cyberpsychology.eu/article/view/4223/3265

Wang, D. (2017). A study of the relationship between narcissism, extraversion, drive for entertainment, and narcissistic behavior on social networking sites. *Computers in Human Behavior*, 66, 138-148.

We Chat Chatterbox (2016, December 29). *The 2016 WeChat Data Report*. Retrieved Nov.2, 2017, from http://blog.wechat.com/2016/12/29/the-2016-wechat-data-report/

Westin, A. F. (1967). *Privacy and freedom*. Atheneum, New York.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6), 2799-2816.

Yoon, C., Hwang, J. Kim, R. (2012). Exploring Factors That Influence Students' Behaviors in Information Security. *Journal of Information Systems Education*, 23(4), 407-414.

Youn, S. (2005). Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk–Benefit Appraisal Approach. *Journal of Broadcasting & Electronic Media*, 49, 86-110, doi: 10.1207/s15506878jobem4901_6.

Youn, S. (2009). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *The Journal of Consumer Affairs*, 43, 389-418.

Zhang, L., & McDowell, W. C. (2009). Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce*, 8(3-4), 180-197.