https://doi.org/10.48009/2_iis_2016_56-64

Issues in Information Systems
Volume 17, Issue II, pp. 56-64, 2016

CONSUMER ADOPTION AND USE OF MOBILE APPLICATIONS: DO PRIVACY AND SECURITY CONCERNS MATTER?

Gary Garrison, Belmont University, gary.garrison@belmont.edu
Sang Hyun Kim, Kyungpook National University, ksh@knu.ac.kr
Xiaobo Xu, American University of Sharjah, xiaobo@aus.edu

ABSTRACT

This study examines individuals' security and privacy concerns with their intention to use mobile applications. A research model was developed from the principal tenets of the theory of planned behavior (TPB) and protection motivation theory (PMT) to examine: Do security and privacy concerns impact individuals' intention to use mobile applications? Our analysis shows support for the relationships among predictor variables (attitude, subjective norm, perceived behavioral control, concern for information privacy and perceived vulnerability) and the outcome variable (behavioral intention).

Keywords: Theory of Planned Behavior (TPB), Protection Motivation Theory (PMT), Information Security and Privacy, Perceived Vulnerability

INTRODUCTION

The use of mobile applications to access popular websites and other forms of entertainment has become so ubiquitous and easy to use that most adopters are unaware of the potential vulnerabilities or exactly what they are giving up to download these applications. For mostly free apps, the code inserted by advertisers may introduce vulnerabilities that can be exploited by allowing outsiders access to address books, photos and text messages; an ability to track the device using its GPS; and control of the mobile device itself. Despite the popularity of mobile applications and ease by which individuals can access their favorite web content, it is imperative that adopters are made aware of the potential for loss of privacy, lack of identity protection, and other exploits.

Theoretical Framework

Theory of planned behavior (TPB) proposes that an individual's intention to act is a function of the relevant information, psychological processes, and personally held beliefs germane to one's behavior (Ajzen, 1991). TPB proposes attitude, subjective norm and perceived behavioral control are three conceptually distinct variables that help predict an individual's intention to perform a particular behavior (Ajzen, 1991). These three variables have been shown to capture the motivating factors that influence an individual's behavior such as the amount of effort he/she is willing to exert to perform that behavior, but is also dependent upon other factors such as opportunity, cognitive abilities, available resources and self-efficacy (Ajzen, 1991). Researchers have reported that attitude (e.g., personal motivation), subjective norms (e.g., encouragement from family, friends and peers), and perceived behavioral control (e.g., familiarity and self-efficacy) have a positive and direct relationship with the use of technology (Garrison, Rebman & Kim, 2016). Together, we expect these factors play an important role in predicting the actual use of mobile applications.

An individual's attitude represents his/her favorable or unfavorable evaluation to performing a particular behavior. If an individual's attitude is favorable toward a particular behavior, then he/she believes that it will lead to a positive outcome. According to Ajzen & Fishbein (1980, 2005), attitude is likely formed from the beliefs representing the expected benefits and the perceived risks of using a technology. If a technology (e.g., mobile application) is unfamiliar to an individual and he/she believes the expected benefits will outweigh the perceived risks, then those beliefs are likely to result in a positive attitude toward the mobile application. In contrast, if an individual believes the perceived risks will outweigh the expected benefits, then he/she will likely reject the mobile application. Therefore, we expect a positive relationship between attitude and behavioral intention.

Subjective norm represents the social pressure applied to an individual to engage in a particular behavior (Fishbein & Ajzen, 1975). Subjective norm indicates how an individual is influenced by members of his/her social network, which helps predict whether or not the individual will perform a conforming behavior (Garrison, Rebman, & Kim, 2016). Research shows that an individual's behavior is influenced by a both the beliefs of one's social network and the importance assigned to each opinion (Fishbein, & Ajzen, 1975; 2010). Therefore, subjective norms are shaped by the perceived expectations from one's social network and his/her motivation to please members of this referent group. In other words, the greater the pressure exerted by one's social network to download and use a mobile application, the more likely that individual will comply with the behavior. Therefore, subjective norm should have a positive impact on one's behavioral intention.

Perceived behavioral control, represents an individual's perceptions regarding the difficulty or ease by which he/she can perform a behavior given both the internal and external factors that can influence the outcome (Ajzen, 1991; 2006). According to Ajzen (1991), perceived behavioral control varies depending upon the situation and the behavior being evaluated. To this point, perceived behavioral control may be influenced by one's previous experiences with downloading and using mobile applications, feedback from one's social network regarding a mobile application or some other factor that can alter the relative ease by which an individual can download and use a mobile application. The more opportunities an individual has to engage in a behavior, the more control he/she will gain over that behavior (Ajzen, 1991). Therefore, we expect a positive relationship between perceived behavioral control and behavioral intention.

Protection motivation theory (PMT) is widely used in information security research to predict individuals' intentions to protect themselves upon receiving recommendations that incite fear within those individuals (Boss et al., 2015). PMT's core premise is that an individual's assessment of fear triggers the threat appraisal process. A threat appraisal is comprised of an individual's perceived vulnerability to a threat and the perceived severity of harm caused by the threat (Rogers, 1983). PMT suggests that an individual will invoke protection motivation if the threat and subsequent fear has a heavier weight than the perceived rewards (Boss et al., 2015). A key component of the threat appraisal process is the evaluation of the rewards for not protecting oneself (Rogers, 1983) such as downloading a free mobile application when there is concern for exploitation. If the reward of downloading a mobile application outweighs the perceived threat of exploitation, then an individual will likely choose to download the mobile application rather than engage in a protective behavior. In contrast, a threat and subsequent fear can motivate adaptive behavior such as rejecting the mobile application and/or updating device's software if the individual thinks he/she has the ability to avert the threat to avoid any negative outcomes.

Information privacy refers to an individual's right to control and decide what personal information is shared with others (Bansal et al., 2016). According to Angst and Argarwal (2009), information privacy concern is a psychological construct that captures the extent to which an individual is concerned about his/her ability to control how others collect, store and use personal information. For the purposes of this study, information privacy concern reflects the extent to which an individual is troubled by the information collection practices of mobile application developers and advertisers, and how the information collected will be used. Previous research has shown information privacy concern to be a strong predictor of privacy-related behaviors when examining the motivating factors for individuals to disclose or conceal personal information over the Internet (Stewart & Segars, 2002). Specifically, Dinev et al. (2006) reported that information privacy concerns have a negative impact on an individual's intention to use e-commerce services. Therefore, we expect a similar relationship exists within the context of mobile applications adoption.

Perceived vulnerability refers to the likelihood that an individual will experience harm by engaging in a particular behavior (Sun et al., 2013). According to the protection motivation theory (PMT), an individual's evaluation of the vulnerability and his/her ability to cope with the threat will determine his/her behavior (Rogers, 1975). In other words, if an individual perceives a mobile application to render them vulnerable to an exploit, then he/she will likely avoid the threat and choose not to adopt the application in question. In contrast, if adopting the mobile application leaves the individual with little to no feelings of vulnerability to an exploit, then he/she would likely adopt the mobile application.

RESEARCH METHODOLOGY

This research focuses on the following research question: Do security and privacy concerns impact individuals' intention to use mobile applications?

The research hypotheses are as follows:

H_1: An individual's attitude toward a mobile application is positively related to his/her intention to use it.

H_2: The use of a mobile application by members of an individual's social network is positively related to his/her intention to use it.

H_3: The ease by which an individual can use a mobile application is positively related to his/her intention to use it.

H_4: An individual's concern about how a mobile application allows for the collection, storage and use of personal information is negatively related to his/her intention to use it.

H_5: The level of vulnerability perceived by an individual regarding how a mobile application allows for the collection,
storage and use of personal information is negatively related to his/her intention to use it.

The five hypotheses were tested using an online survey of previously validated measures and modified to fit a mobile application context. Respondents were made up of both graduate and undergraduate students studying in the United States, South Korea and Dubai. A total of 381 students participated in this survey. The breakdown of the respondents by age, gender, education level, ethnicity, hours spent using mobile applications and the activities conducted using mobile applications are shown in Table 1.

Table 1. Demographics

Demographic categories		Frequency	Percentage
Age	≥ 19	95	24.9%
	20 – 29	83	21.8%
	30 – 39	101	26.5%
	40 – 49	88	23.1%
	50+	14	3.7%
Gender	Male	208	54.6%
	Female	173	45.4%
Level of Education	High school grad	25	6.6%
	Freshman	28	7.3%
	Sophomore	31	8.1%
	Junior	43	11.3%
	Senior	20	5.2%
	College Undergraduate Degree	106	27.8%
	Associates Degree	19	5.0%
	Graduate Degree	95	24.9%
	Professional Degree	14	3.7%
	Asian	165	43.3%
	White	88	23.1%
	Middle Eastern	52	13.6%
	European	65	17.1%
	Other	11	2.9%
Hours spent on Mobile Apps	>1	37	9.7%
	1 – 3 hours	154	40.4%

	4 – 6 hours	119	31.2%
	7 – 9 hours	60	15.7%
	9+ hours	11	2.9%
Activities of Mobile Apps. (Multiple Responses)	School or Work	287	75.3%
	Gaming	219	57.5%
	Social Media	315	82.7%
	Shopping	257	67.5%
	News and Other Entertainment	205	53.8%
	Banking and Finance	219	57.5%

RESULTS

CFA and Internal Consistency

Confirmatory factor analysis (CFA) was conducted to test the validity of the measurement model using AMOS 22.0. First, the overall fitness was examined to purify the measurement model. Several indices, including NFI, GFI, AGFI, CFI, RMSEA, and the relative chi-square (χ^2/df) was used as a guideline for evaluating the model's fit. Fit is demonstrated by testing to see if the threshold of NFI, GFI, and CFI is at least 0.9, AGIF is at least 0.8 (Bentler, 1990) and RMSEA less than 0.07 (Steiger, 2007). In addition, the relative χ^2 (χ^2/df) should have range from 3 to 5.

The initial test (Model 1) used a total sample of 381 with 29 items. The results showed that three indices (NFI, GFI, and CFI) were below the threshold and the modification index (MI) indicated that two items (cip1 and pbs5) had a cross-loading issue, indicating that these variables loaded on other latent variables. Therefore, these two items were dropped from the model and the measurement model (Model 2) was re-evaluated for fit. Table 2 shows the results of the overall fit, which indicates all of Model 2's indices exceeded the recommended threshold.

Table 2. Goodness of Fit

	NFI	**GFI**	**AGFI**	**CFI**	**RMSEA**	***X²/df***
Model 1	0.845	0.884	0.812	0.891	0.049	2.128
Model 2	0.905	0.927	0.859	0.937	0.041	1.952
Threshold	≥ 0.9	≥ 0.9	≥ 0.8	≥ 0.9	≤ 0.05	≥ 3.0

Note: cip1and pbc5 dropped from further analysis

Next, the measurement model's convergent validity, discriminant validity and internal consistency were examined using individual item loading, average variance extracted (AVE), and reliability, respectively. The factor loadings from the CFA test showed that all of the items loaded onto their respective latent variables and had loadings ranging from 0.709 to 0.839, demonstrating convergent validity. In addition, the research model's internal consistency was evaluated using Cronbach's Alpha for each variable in the model. The alphas ranged from 0.792 to 0.938, which exceeds the recommended threshold of 0.7, meaning the measurement model was shown to be reliable. Table 3 displays the results of the convergent validity and internal consistency tests.

Table 3. Convergent Validity and Internal Consistency Tests

Construct	Item	Loadings	t-value	AVE	Cronbach's Alpha
Attitude	att1	0.832	20.03	0.627	0.889
	att2	0.827	16.63		
	att3	0.790	15.10		
	att4	0.751	16.36		
	att5	0.754	10.69		
Subjective Norm	sn1	0.709	17.16	0.571	0.894
	sn2	0.717	13.31		
	sn3	0.835	16.49		
Perceived Behavioral Control	pbc1	dropped		0.592	0.816
	pbc2	0.779	12.67		
	pbc3	0.760	14.59		
	pbc4	0.723	15.45		
	pbc5	0.814	18.09		
Concern for Information Privacy	cip1	0.728	10.03	0.638	0.792
	cip2	0.764	16.13		
	cip3	dropped			
	cip4	0.808	12.16		
	cip5	0.825	15.47		
	cip6	0.861	17.27		
Perceived Vulnerability	pv1	0.832	16.68	0.621	0.853
	pv2	0.739	13.11		
	pv3	0.747	12.65		
	pv4	0.830	15.70		
Behavioral Intention	bi1	0.800	19.58	0.592	0.922
	bi2	0.726	14.49		
	bi3	0.781	11.79		
Use Behavior	ub1	0.836	19.15	0.641	0.938
	ub2	0.798	15.86		
	ub3	0.766	13.48		

Finally, the measurement model was evaluated for discriminant validity. Discriminant validity evaluates whether or not constructs are significantly different from one another. To demonstrate discriminant validity, the correlation among constructs should be smaller than the square root of AVE for each construct (Chin, 1998). As shown in Table 4, the measurement model meets the requirement for discriminant validity, since the square root of AVE (the items in bold) exceeds the correlations in each column and row.

Table 4. Discriminant Validity Test

Construct	1	2	3	4	5	6	7
1. Attitude	**0.792**						
2. Subjective Norm	0.217	**0.756**					
3. Perceived Behavioral Control	0.323	0.261	**0.770**				
4. Concern for Information Privacy	0.309	0.238	0.307	**0.799**			
5. Perceived Vulnerability	0.275	0.405	0.354	0.358	**0.788**		
6. Behavioral Intention	0.259	0.360	0.352	0.299	0.440	**0.770**	
7. Use Behavior	0.334	0.372	0.289	0.416	0.351	0.320	**0.801**

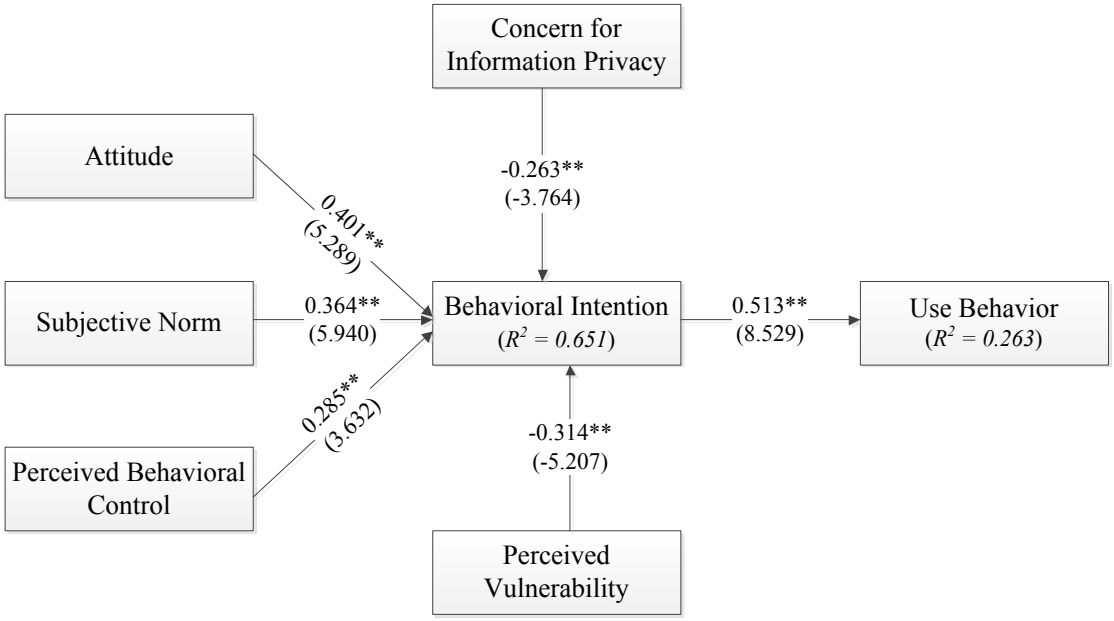
Analysis of Structural Model

The proposed hypotheses were tested by formulating a structural equation model (SEM) with AMOS 22.0. The SEM test, not only provides the standardized coefficient (β), but also, the squared multiple correlation (R^2). The standardized coefficient (β), along with its corresponding p-value, indicate the strength of the causal relationships between two constructs (Wixom & Watson, 2001), which determine whether or not to accept the hypotheses. The squared multiple correlation (R^2) provides the amount of variance in each endogenous variable that can be explained by the exogenous variables.

The results of the structural model shows support for all of hypotheses (see Figure 1). First, the path coefficient (β =0.402) between Attitude and Behavioral Intention is significant at $p<0.01$. Similarly, Subjective Norm and Perceived Behavioral Control were significantly related to Behavioral Intention (β = 0.364 and β = 0.285, respectively) at $p<0.01$. Thus, H1, H2 and H3 were supported. Our findings demonstrate that the principle tenets of TPB hold true for users' intentions to use mobile applications given they have a positive attitude toward the mobile application, are provided support/pressure from their social network to use the mobile application, and they perceive it to be easy to download and use the mobile application given their prior experiences.

Next, H4 and H5 stated negative relationships between Concern for Information Privacy and Perceived Vulnerability on Behavioral Intention. Both hypotheses were supported with the path coefficient (β =-0.263) and (β = -0.314), respectively. The support for H4 and H5 would suggest that individuals' intention to download and use a mobile application is negatively impacted when they are concerned for their privacy or perceive themselves vulnerable to potential exploitation by unauthorized individuals. Finally, H6 stated a positive relationship between Behavioral Intention and Use Behavior, which was supported with the path coefficient (β =0.513) at $p<0.01$. This finding supports previous TPB research that have demonstrated a positive correlation between intent and actual behavior. Specifically, our results suggest that respondents who report intent to download and use a mobile application will actually follow through on that intent. Table 5 summarizes the test results for each hypothesis.

The final test conducted was the evaluation of the R^2 of each endogenous variable (Behavioral Intention and Use Behavior). Five exogenous variables (Attitude, Subjective Norm, Perceived Behavioral Control, Concern for Information Privacy, and Perceived Vulnerability) explained approximately 65.1% of the variance in Behavioral Intention. Similarly, Behavioral Intention explained approximately 26.3% of variance in Use Behavior. These findings empirically validate the principle tenets of TPB. Attitude, Subjective Norm and Perceived Behavioral Control are shown to be important factors impacting individuals' Behavior Intention to download and use mobile applications. The results also show that individuals' concerns over privacy and vulnerability to exploitation negatively impact their behavioral intent. The latter may help explain why the model only contributes 26.3% of respondents use behavior.



Notes: X^2/df = 1.862, NFI = 0.918, GFI = 0.905, AGFI = 0.873, CFI = 0.929, RMSEA = 0.035,
**: p<0.01

Figure 1. The Structural Model

Table 5. Summary of Hypothesis Tests

Hypothesis	Path	Std. β	t-value	Result
H1	Attitude → Behavioral Intention	0.402	5.289	S**
H2	Subjective Norm → Behavioral Intention	0.364	5.940	S**
H3	Perceived Behavioral Control → Behavioral Intention	0.285	3.632	S**
H4	Concern for Information Privacy → Behavioral Intention	-0.279	-3.884	S**
H5	Perceived Vulnerability → Behavioral Intention	-0.314	-5.207	S**
H6	Behavioral Intention → Use Behavior	0.513	8.529	S**

Note: **: p<0.01, S: Supported

SUMMARY

The objective of this paper was to evaluate whether or not individuals' concerns regarding information privacy and perceived vulnerability impact their intention to download and use mobile applications. The research model demonstrates that the principle tenets of TPB still hold true for individuals who intend to use mobile applications. However, attitude, subjective norm and perceived behavioral control may be tempered by individuals' concern over their information privacy and perceived vulnerability with respect toward the potential exploitation by unauthorized individuals. It may be that more experienced users are able to employ tactics that help prevent against unauthorized access to their data and other exploits, or it may be that adopters are unaware or naive to the notion that they render themselves vulnerable when downloading free mobile applications. Consistent with previous research, we hypothesized and found a direct and negative relationship between concern for information privacy and perceived vulnerability on behavioral intention. By bringing behavioral intention in line with concern for information privacy and perceived vulnerability to potential exploitation, it may be that as individuals felt a heightened sense of vulnerability or loss of privacy, they would take more preventive measures to avoid the potential exploitations. These preventative measures could include providing false information upon registration, updating their software, or

avoid adopting the mobile application altogether. This may help explain why the research model only explained 26.3% of individuals' use behavior despite its ability to predict 65.1% of behavioral intention. These findings may suggest that individuals' concern over information privacy and perceived vulnerability have some influence on the predictive power of TPB. Future studies need to be conducted to explore these relationships more deeply or identify new relationships that might help explain why individuals use mobile applications.

Our results should be interpreted based on methodological approach used in this research. First, data was collected using an online, cross-sectional survey design. Second, the 381 respondents were made up of a convenience sample of both graduate and undergraduate students. However, the respondents were studying at a university located in either the United States, South Korea or Dubai, which should help with the generalizability of the study.

REFERENCES

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), 179-211.

Ajzen, I., & Fishbein, M. (2005). The influence of attitudes on behavior. In D. Albarracín, B. T. Johnson, & M. P. Zanna (Eds.), The handbook of attitudes (pp. 173-221). Mahwah, NJ: Erlbaum.

Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behavior. Englewood Cliffs, NJ: Prentice-Hall.

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly, 33*(2), 339-370.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management 53,* 1-21.

Bentler, P. M. (1990). Comparative fit indexes in structural models. *Psychological Bulletin, 107*, 238-246.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837-864.

Chin, W. (1998). The partial least squares approach for structural equation modeling. in G. A. Marcoulides (Ed.), Modern methods for business research (pp. 295–236). London: Lawrence Erlbaum Associates.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., and Colautti, C. (2006). Privacy calculus model in e-commerce–a study of Italy and the United States. *European Journal of Information Systems*, *15*(4), 389-402.

Fishbein, M., & Ajzen, I. (2010). Predicting and changing behavior: The reasoned action approach. New York: Psychology Press (Taylor & Francis).

Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention, and behavior: An introduction to theory and research. Reading, MA: Addison-Wesley.

Garrison, G., Rebman, C., & Kim, S. (2016). An identification of factors motivating individuals' use of cloud-based services. *Journal of Computer Information Systems,* (forthcoming).

Goodhue, D. L. (1995). Understanding user evaluations of information systems. *Management Science, 41*(12), 1827-1844.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology: Interdisciplinary and Applied*, *91*(1), 93-114.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation," In J. Cacioppo and R. E. Petty (Eds.), Social psychophysiology (pp. 153-176). New York: The Guilford Press.

Steiger, J. H. (2007). Understanding the limitations of global fit assessment in structural equation modeling. *Personality and Individual Differences*, *42*(5), 893-98.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research, 13*(1) 36-49.

Sun, Y., Wang, N., Guo, X., & Peng, Z. (2013). Understanding the acceptance of mobile health services: A comparison and integration of alternative models. *Journal of Electronic Commerce Research, 14*(2), 183-200.

Wixom, B. H. & H. J. Watson (2001). An empirical investigation of the factors affecting data warehousing success. *MIS Quarterly, 25*(1), 17-38.