8-2010

Risky Behavior in Online Social Media: Protection Motivation and Social Influence

M. Shane Banks
University of Memphis, msbanks@memphis.edu

Colin G. Onita
University of Memphis, cgonita@memphis.edu

Thomas O. Meservy
University of Memphis, tmeservy@memphis.edu

Risky Behavior in Online Social Media: Protection Motivation and Social Influence

M. Shane Banks[1]
University of Memphis
msbanks@memphis.edu

Colin G. Onita
University of Memphis
cgonita@memphis.edu

Thomas O. Meservy
University of Memphis
tmeservy@memphis.edu

ABSTRACT

Online Social Media (OSM) websites have attracted millions of users by enabling them to socially interact in ways that were not possible before. While the explosion of OSM use has had many benefits, it also has a darker side where an individual's personal information can potentially be misused. This study develops and tests an empirical model based on a theoretical lens provided by Protection Motivation Theory (PMT) to examine the salient factors that influence an individual's perceptions of threat and their intention to use OSM websites. We investigate this model with a data set representing survey responses from 197 OSM users. Results suggest that rewards, which are largely overlooked in the IS PMT literature, are the primary influence in the perceived threat calculation in the OSM context. In addition, social influence was found to significantly influence behavioral intentions to share information on OSM websites.

Keywords

Online social media, protection motivation, social influence, social networking

INTRODUCTION

Beware what you share! Sharing information on Online Social Media (OSM) websites such as Facebook, Twitter, MySpace or YouTube can cost you your job, your money, your marriage or even your freedom. The popular press is full of examples of unwary users who have posted personal information online only to realize too late that their information had fallen into the wrong hands. An employee for a major healthcare company was fired for posting information that the company considered a violation of company policy, a British citizen was awarded $44,000 after suing someone who had posted false information about them, suspicious spouses are combing OSM websites for incriminating information that has been used as evidence in divorce proceedings, and law enforcement agencies are using information obtained from Facebook and MySpace to track down and prosecute criminals. To raise awareness of the risks of posting personal information online, websites such as www.pleaserobme.com have created websites that aggregate tweets from users that let the world know that they are no longer at home.

For the purpose of this research OSM websites are defined as web-based platforms which allow individuals to interact and share information, opinions, insights, experiences, and perspectives with others. OSM websites have continued to experience exponential growth fueled by individual's desire to share information and stay connected with others. Facebook alone boasts over 400 million active who contribute more than 5 billion pieces of content per day[2]. The online social tools provided by these OSM websites enable users to engage in social activities and information sharing in many new, interesting and user friendly ways which have enabled them to attract and sustain a huge following.

The proliferation of OSM websites has also had a darker side in that the personal information shared by individuals on these websites has, in some cases, been misused with dire consequences for the information provider or others identified in that information. Although most users are generally aware of the potential risks of posting personal information and content on OSM websites, some OSM users still knowingly post sensitive and personal information that can be used in detrimental

[1] All authors contributed equally to this work

[2] http://www.facebook.com/press/info.php?statistics

ways. Many users often mistakenly rely on the ever changing security policies of OSM websites or trust their circle of friends to protect their privacy.

Past literature on electronic information sharing focuses primarily on the motivations for sharing information in organizational knowledge management systems (Bock, Zmud, Kim and Lee, 2005; Kankanhalli, Tan and Wei, 2005), and within designated communities of practice (Ma and Agarwal, 2007; Wasko and Faraj, 2005) or on work related wikis within professional associations (Kane and Fichman, 2009). However, little research has focused on investigating why individuals would knowingly engage in a potentially risky information sharing behavior on OSM websites. This paper seeks to fill this gap in the literature by providing an empirical investigation of potentially risky information sharing behaviors utilizing OSM.

We examine information sharing behavior on OSM websites through the theoretical lens of Protection Motivation Theory enhanced by behavioral constructs adapted from literature on social influence. The purpose of this study is to examine the affect of an individual's perception of threat as well as the effect of social influence on information sharing behavior on OSM websites. Therefore, the primary research questions we seek to answer in this study are:

- What are the salient factors that influence an individual's perceptions of threat in their intention to use OSM websites?
- How does social influence affect behavioral intentions of information sharing on OSM websites?

The remainder of this paper is organized as follows. First, the theoretical background will be presented followed by the development of our research model and hypotheses. Next, we offer an in-depth description of our research methodology and conclude with our results, discussion, limitations and implications.

THEORETICAL BACKGROUND

Protection Motivation Theory

Protection Motivation Theory (PMT) (Rogers, 1975; Rogers, 1983) provides a lens to examine individual behaviors as a person confronts a potentially threatening situation. PMT has received significant empirical support in assessing individual's willingness to adopt particular technology related behaviors to avoid potential negative consequences (Herath and Rao, 2009; Johnston and Warkentin, 2010; Stafford and Poston, 2010). According to PMT, behavior is influenced by an individual's threat and coping appraisals concerning the potential threat.

Threat assessment is the individual's overall perception of the danger of the situation and consists of three dimensions: perceived severity, perceived vulnerability and rewards (Rogers and Prentice-Dunn, 1997). PMT theorizes that prior to engaging in an activity an individual makes a cognitive assessment of the potential threat of the activity. This threat assessment may be the result of a cognizant and purposeful evaluation or it may be the result of an implicit evaluation process. PMT suggests that the threat assessment of a particular activity or situation results from a cognitive subjective calculation:

Threat Assessment = Perceived Vulnerability + Perceived Severity - Rewards

PMT has primarily been used in the MIS literature to examine phenomena such as employee's response to organizational security policies (Herath and Rao, 2009), individual use of security software (Johnston and Warkentin, 2010; Stafford and Poston, 2010) or implementation of home wireless security (Woon, Tan and Low, 2005).

RESEARCH MODEL AND HYPOTHESES

Building on the tenets of Protection-Motivation Theory we provide an integrated framework that explains potentially risky online information sharing behavior. The core of our model is based on the PMT threat assessment calculation which is a trade-off between the perceived vulnerability and severity of a threat versus the perceived rewards associated with a risky behavior (Rogers and Prentice-Dunn, 1997). The behavioral intention we examine in our study is a user's intention to share or not share information on OSM websites by current users of those websites. Since these are users currently using the technology, our study examines the threat assessment without considering the efficacy of the user in their ability to share or not share information.

The first component of the threat assessment calculation is the perceived severity of the threat associated with sharing personal information on OSM websites. Perceived severity is an individual's perception of the extent or level of potential

damage which may result from engaging in the information sharing activity (Rogers and Prentice-Dunn, 1997). Prior literature shows that as an individual's perception of the severity of a threat increases, their assessment of that threat also increases (Johnston and Warkentin, 2010; Rogers and Prentice-Dunn, 1997; Stafford and Poston, 2010; Woon et al., 2005). An individual's appraisal of the severity of the threat associated with sharing information on OSM websites is directly linked to the sensitivity of the information that is being shared. If an individual considers that sharing a piece of personal information on an OSM website will have severe negative consequences then the potential threat represented by sharing that information will higher.

Therefore, we hypothesize:

H1: Perceptions of increased severity of sharing personal information on OSM websites will positively influence an individual's associated perceived threat assessment.

The second component of the threat assessment calculation is the perceived vulnerability associated with sharing personal information on OSM websites. Perceived vulnerability is the individual's perception of their likelihood of experiencing negative consequences from sharing personal information on OSM websites. As an individual perceives that their vulnerability to a threat increases, their perception of the threat will also increase (Johnston and Warkentin, 2010; Rogers and Prentice-Dunn, 1997; Stafford and Poston, 2010; Woon et al., 2005). In the OSM setting, as individuals become increasingly aware of the likelihood that posting personal information may have negative consequences for them, their threat assessment will increase.

There, we hypothesize:

H2: Perceptions of increased vulnerability of sharing personal information on OSM websites will positively influence an individual's associated perceived threat assessment.

The last component of the threat assessment calculation is the perceived rewards associated with the OSM information sharing behavior. Rewards are the positive or desirable consequences that result from engaging in an activity. PMT (Rogers and Prentice-Dunn, 1997) describes this as the benefits that an individual obtains from engaging in a potentially risky behavior. Rewards in the OSM context includes utilitarian rewards such as the ability to accomplish a task with fewer resources, hedonic rewards such as enjoyment and fun (Babin, Darden and Griffin, 1994; Hirschman and Holbrook, 1982) and from increased ability to communicate and engage in relationships with other individuals who share common goals, values and activities (Deci and Ryan, 2002). PMT proposes that rewards negatively influence the perceived level of threat associated with an activity (Rogers, 1983). In examining PMT in security-related technology contexts, the IS literature has largely overlooked this aspect of PMT. In the OSM context, we consider rewards to be a very important factor that influences the appraisal of an individual on the level of threat associated with posting personal information online. In fact, we expect that due to the social nature of OSM websites, rewards are the most significant driver of the threat assessment calculation.

Therefore, we hypothesize:

H3: Perceptions of increased rewards associated with sharing personal information on OSM websites will negatively influence an individual's associated perceived threat assessment.

Threat Assessment

PMT is based on a simple but powerful concept which theorizes that an individual performs a mental calculation when he or she engages in a potentially risky behavior (Rippetoe and Rogers, 1987; Rogers and Prentice-Dunn, 1997). This calculation is a trade-off between the rewards that result from engaging in the risky behavior and the perceived vulnerability of the individual to the threat plus the perceived severity of the consequences when and if the threat is realized. In the case of OSM websites, individuals take into consideration the utilitarian, hedonic and social rewards associated with posting personal information and weigh them against the likelihood that the information will be misused and the severity of the consequences resulting from their personal information being misused. This calculation results in a perceived threat assessment which negatively influences their behavioral intentions regarding posting personal information on OSM websites. If the individual perceives the threat of posting personal information is high enough, then they will refrain from posting such information.

Therefore, we hypothesize:

H4: Perceived threat will negatively influence the behavioral intention of an individual to post personal information on OSM websites.

Social Influence

Social influence is another important variable that determines an individual's intention to post personal information on OSM websites. Social influence is the degree to which the individual perceives that his or her social circle and other actors whose opinions matter will support and encourage the information sharing behavior (Hartwick and Barki, 1994; Venkatesh, Morris, Davis and Davis, 2003). Social influence has been shown to be an important factor influencing how individuals use technology (Johnston and Warkentin, 2010). Venkatesh and Davis 2000 (pg. 451) describe social influence in a technology use setting as "the explicit or implicit notion that the individual's behavior is influenced by the way in which they believe others will view them as a result of having used the technology."

In other contexts, social influence was defined as social norm, and was shown to be a significant determinant of behavioral intentions (Ajzen, 1991; Fishbein and Ajzen, 1975; Venkatesh et al., 2003). Another interesting aspect of social influence is that it bolsters the image (Moore and Benbasat, 1991) of an individual, which refers to an individual's perception that engaging in the information sharing behavior will enhance his or her social standing within a certain social group.

Social influence may induce an individual to share information on OSM websites even though the individual may consider such a behavior to be potentially threatening or damaging.

Therefore, we hypothesize:

H5: Social influence will have a positive effect on an individual's intentions to post personal information on OSM websites.

Realized threat is the conceptualization of an individual's prior experience with a particular threat. In his extension of the original PMT, Rogers (1983) theorized that an individual's previous exposure to a threat would significantly influence the cognitive evaluation of the threat and the threat's impact on future behavior. In the OSM context, realized threat is the individual's actual experience of negative consequences from online information sharing behavior. We theorize that an individual that has experienced a realized threat in their information sharing activities will utilize that past experience in their threat assessment and, specifically, will impact their perceived vulnerability to the threat.

Therefore, we hypothesize:

H6: Realized threat will have a positive effect on an individual's perceived vulnerability to a potential threat in the context of information sharing on OSM websites.

Figure 1 illustrates the research model and associated hypotheses and expected directionality of the effects.

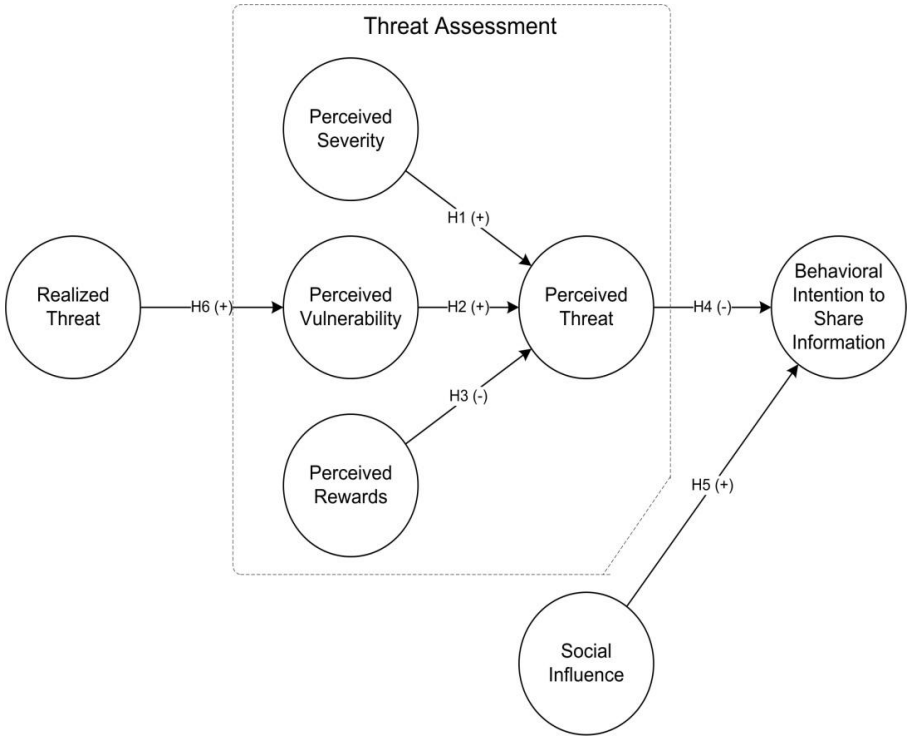

Figure 1 - Research model and hypotheses

RESEARCH METHODOLOGY

To empirically test the relationships proposed by our model, we chose to employ a field study using survey methodology. In accordance with the guidelines presented by Straub (1989) we employed previously validated scales where possible. Our survey instrument was primarily adapted from instruments used in various studies that investigated the impact of PMT or social influence on individual behavioral intentions. The survey measured seven primary constructs and four control variables. The primary constructs are: Behavior Intent (INT), Social Influence (SI), Perceived Threat (PT), Perceived Severity (SEV), Perceived Vulnerability (VUL), Perceived Rewards (REW) and Realized Threat (RTH). The primary constructs were all measured via multiple items using seven-point Likert scales. INT and SI were adapted from Venkatesh et al. (2003) and Johnston and Warkentin (2010). PT, SEV, and VUL were adapted from Johnston & Warkentin (2010) and Woon et al. (2005). REW was adapted from Arnould (2003) and Deci and Ryan (2002) and RTH items were self developed. Content validity was established through both extensive literature review and a content validity expert panel comprised of faculty members and doctoral students adept in quantitative survey research methodology. The survey items are listed in Appendix A.

In following with PMT, PT was modeled as a second order formative construct (Rippetoe and Rogers, 1987; Rogers and Prentice-Dunn, 1997). To facilitate model identification, we used a one item reflective measure for the PT construct as suggested by Edwards and Bagozzi (2000). Given that PMT describes a mental calculation when evaluating PT (Rippetoe and Rogers, 1987; Rogers and Prentice-Dunn, 1997), we used three unique items (measuring perceived severity, perceived vulnerability and perceived reward individually) to calculate PT.

The survey was administered to a sample of probable social media website users. Participants were drawn from students enrolled in business courses at two universities located in the central United States. Motivation to participate in the survey was provided through two different mechanisms: 1) a random drawing to receive a $25 gift card to a national retail store for those who completed the survey, and 2) extra credit from the instructor for specific participating classes. Prospective participants were contacted via email with details of the study, benefits, and risks. The survey was hosted online and required approximately ten minutes to complete.

Invitations to participate were sent to 564 students. 249 initiated the survey and ultimately 197 completed the survey for an effective response rate of 34.9%.

Data Analysis

Partial least squares (PLS) was the data analysis technique utilized in the study and was used to assess the measurement model and also the structural model for our research hypotheses. SmartPLS (Ringle, Wende and Will, 2005) was used to conduct the analysis. Throughout the analysis, we followed the recommendations of Straub (1989) and Straub, Boudreau, and Gefen (2004), particularly as they apply to validity.

Construct validity refers to how well item measures correlate with a theoretical construct. In this study we specifically look at two aspects of construct validity: namely convergent validity and discriminant validity.

Convergent validity is demonstrated when each of the measurement items loads with a significant t-value on its latent construct (Gefen and Straub, 2005). Table 1 indicates the outer model loadings, along with the t-values. The t-values were estimated using a nonparametric bootstrapping procedure using 1000 samples (Chin, 1998). The loadings for all constructs are significant at $\alpha = 0.05$ significance level and uniformly high (above 0.7) with a majority above 0.85, attesting to convergent validity.

Item	Item Loading	T-Statistic	Item	Item Loading	T-Statistic
INT1	0.971	144.936	**SEV1**	0.901	38.497
INT2	0.972	141.214	**SEV2**	0.912	61.464
INT3	0.979	189.651	**SEV3**	0.811	19.043
RTH1	0.914	32.001	**SI1**	0.853	24.169
RTH2	0.892	25.027	**SI2**	0.893	47.480
RTH3	0.882	27.312	**SI3**	0.905	57.248
REW1	0.891	61.162	**SI4**	0.883	41.231
REW2	0.854	27.844	**VUL1**	0.784	17.119
REW3	0.914	60.110	**VUL2**	0.877	40.989
REW4	0.825	21.849	**VUL3**	0.878	39.267

Table 1 - Significance test of measurement item loadings

Discriminant validity exists when the item measures load highly on the appropriate theoretical construct and not highly on other factors (Gefen and Straub, 2005). Additionally, establishing discriminant validity in PLS also requires an appropriate Average Variance Extracted (AVE) analysis. AVE captures the variance of the items associated with a latent construct. Gefen and Straub (2005) suggest that the "square root of the 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 .50." Table 2 displays the square root of the AVE for each construct (on the diagonal) and also the correlation between constructs. The data suggest that these conditions are met and thus suggest appropriate discriminant validity.

	INT	PT	RTH	REW	SEV	SI	VUL
INT	**0.974**						
PT	-0.333	**1.000**					
RTH	-0.017	0.005	**0.896**				
REW	0.641	-0.497	0.103	**0.872**			
SEV	-0.108	0.442	0.038	0.008	**0.876**		
SI	0.336	-0.222	0.218	0.557	0.103	**0.884**	
VUL	-0.134	0.537	0.214	-0.034	0.503	0.066	**0.848**

Table 2 - Square root of AVE scores and correlation of latent variables

Table 3 summarizes results for structural model constructs. Cronbach's α is used to measure the internal consistency of item measures. Nunnally (1978) suggests that values should exceed 0.7. If parameter estimates are assumed to be accurate, composite reliability is considered a closer approximation of reliability. Straub et al. (2004) suggest that composite reliability scores should exceed 0.8. A more conservative measure of reliability, AVE, should exceed 0.5 (Straub et al., 2004). Together, the data for these statistics attest to the reliability of the instrument as all recommendations are exceeded in our dataset.

	Cronbach's Alpha	Composite Reliability	AVE
INT	0.972769	0.982162	0.948331
RTH	0.878275	0.924403	0.80303
REW	0.894547	0.926592	0.759641
SEV	0.847632	0.907934	0.76723
SI	0.908274	0.934471	0.781028
VUL	0.804921	0.884129	0.718333

Table 3 - Summary of results for the inner model constructs

Results

The results of our hypotheses testing are shown in Figure 2, which illustrates the structural model with the R^2 value for each of the endogenous constructs. The path coefficients for the inner model are displayed and significant paths are shown with solid lines.

Our results show that 32.1% of the variance in behavioral intentions to post personal information on OSM websites is explained by the factors presented in our model. Also, the antecedents of Perceived Threat proposed by our model explain 56.3% of the variance of this construct. Finally, realized threat, even though it explains only 4.6% of the variance of Perceived Vulnerability, is a significant predictor of Perceived Vulnerability ($p<.01$, $t=3.17$) thus supporting hypothesis 6.

In agreement with PMT and the first three hypotheses, Perceived Severity ($p<.01$, $t=3.60$), Perceived Vulnerability ($p<.01$, $t=7.32$) and Perceived Rewards ($p<.01$, $t=10.02$) all have a significant impact on the perceived threat associated with posting

personal information on OSM websites. Furthermore, while Perceived Severity and Perceived Vulnerability positively influence Perceived Threat, Perceived Rewards exercises a negative influence on this construct. Therefore, hypotheses 1, 2 and 3 are supported.

As expected, the Perceived Threat ($p<.05$, $t=2.57$) associated with posting personal information on OSM websites negatively influences the behavior intention to share personal information on OSM websites. Therefore, hypothesis 4 was supported.

Finally, Social Influence ($p<.05$, $t=2.40$) was also found to have a significant, positive impact on behavioral intentions to share personal information on OSM websites and, therefore, hypotheses 5 was supported.

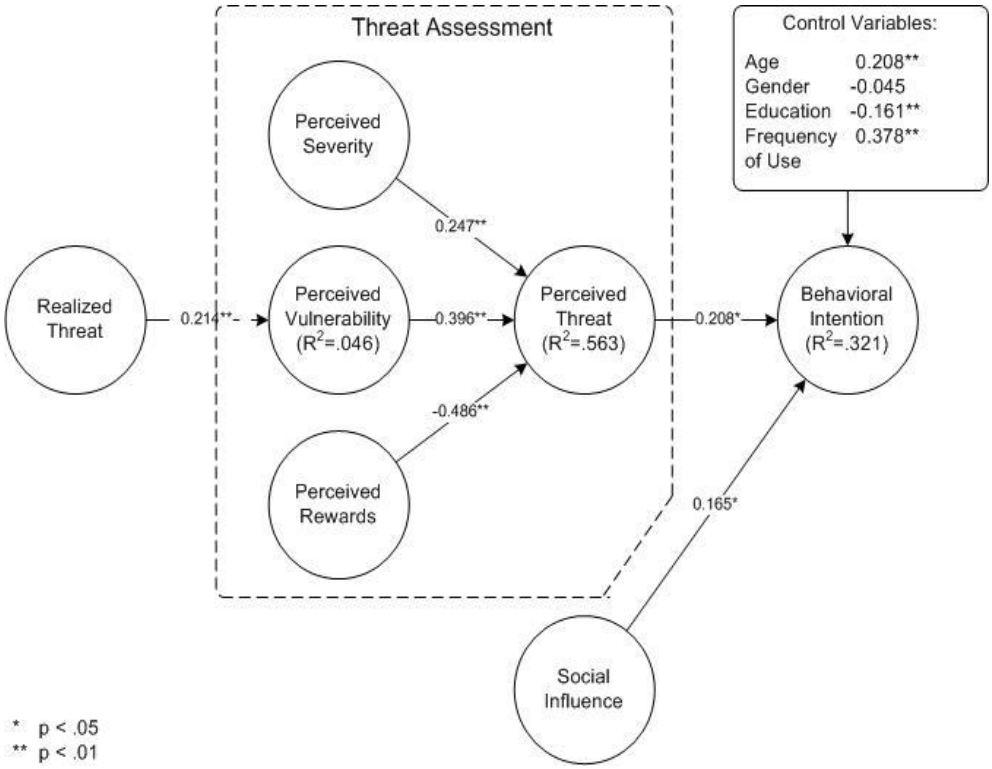

Figure 2 - Structural model including supported hypotheses

DISCUSSION AND CONTRIBUTIONS

This research has several important theoretical and practical implications. This paper elucidates the salient factors that influence an individual's perceptions of threat in their intention to use OSM websites. In accordance with PMT, this paper investigates how individuals perform a mental calculation when engaging in a potentially risky behavior whereby they calculate the trade-off between the potential severity and vulnerability of the threat with the rewards associated with the behavior. In the context of OSM websites, this paper also finds that the vulnerability assessment of a threat is important in constructing an individual's perception of the threat. This finding is in contrast with much of the prior IS PMT literature which found vulnerability to be insignificant in the context of security related policies and products.

In addition, the investigation of the impact of rewards in the PMT threat assessment framework has largely been overlooked in the IS literature. Our research shows that in the context of OSM websites, rewards are the most important factor influencing the threat assessment. As PMT theorizes, perceived rewards neutralize much of the effect of perceived severity and perceived vulnerability resulting in a lower threat assessment and hence a greater likelihood of engaging in the behavior. In addition, our research shows that realized threat is a significant predictor of an individual's perceived vulnerability to a particular threat.

Another important contribution of our research is our finding that social influence is a significant predictor of intention in the OSM context. This is an interesting finding because the TAM literature has often found that social influence is not

significant in voluntary contexts (Venkatesh et al., 2003). Also, while we show that social influence has explanatory power in predicting intention in the OSM context, we find that its influence is less than that of perceived threat.

An interesting result was that one of our control variables - education - had a significantly negative influence on behavioral intentions. This along with the finding that rewards are overriding perceived severity and perceived vulnerability in the threat assessment can inform practice that educating individuals about the risks associated with posting personal information on OSM websites can potentially reduce the number of incidents where this information is misused. Additionally, as expected, one of the greatest predictors of future behavior is current behavior; thus frequency of use of OSM websites significantly predicts behavioral intention. The data also suggest that the age of an individual impacts the behavioral intention to post. However, counter to common intuition, the data suggest that as age increases, so does the likelihood of the intention to post on social media websites. This finding merits additional validation and investigation in future studies.

Like most research, this research does have some limitations. Although we feel strongly that our sample appropriately represents the domain of OSM users, our convenience sample may not generalize well to other populations. Additionally, we do not investigate the self efficacy of an individual to deal with the threat. Self efficacy has been investigated in other PMT studies, but we deemed it not applicable given the setting and the type activity involved (posting or not posting information). This can be a potentially fruitful area for future research that would investigate the influence of self efficacy and other variables on behavioral intentions in an OSM context. In the context of information sharing in online social media, we assert that behavioral intention to post information is predictive of actual behavior, however, we recognize that some recent research suggests that behavioral intentions may not predict actual behavior in certain risk-related contexts (Acquisti and Grossklags, 2005; Hoadley, Xu, Lee and Rosson, 2010).

CONCLUSION

Hundreds of millions of users are flocking to OSM websites like Facebook, MySpace, YouTube and Twitter, many of which are sharing personal information that could possibly be used in a way which could harm them. By examining this phenomenon through the theoretical lens of PMT we find empirical support for the cognitive threat assessment process in the OSM context and that perceived threat and social influence are significant predictors of intention.

REFERENCES

1. Acquisti, A., and Grossklags, J. (2005) Privacy and Rationality in Decision Making, *IEEE Security and Privacy* (January/February), 26-33.
2. Ajzen, I. (1991) The theory of planned behavior, *Organizational behavior and human decision processes*, 50, 2, 179–211.
3. Arnould, E. J., & Thompson, C. J. (2005) Consumer culture theory (CCT): Twenty years of research, *Journal of Consumer Research*, 31, 868–882.
4. Babin, B. J., Darden, W. R., and Griffin, M. (1994) Work and/or fun: measuring hedonic and utilitarian shopping value, *Journal of consumer research*, 20, 4, 644.
5. Bock, G. W., Zmud, R. W., Kim, Y. G., and Lee, J. N. (2005) Behavioral intention formation in knowledge sharing: Examining the roles of extrinsic motivators, social-psychological forces, and organizational climate, *MIS Quarterly*, 29, 1, 87–111.
6. Chin, W. W. (1998) Issues and opinion on structural equation modeling, *Management Information Systems Quarterly*, 22, 1, 7–16.
7. Deci, E. L., and Ryan, R. M. (2002) Handbook of self-determination research, Univ of Rochester Pr.
8. Edwards, J. R., and Bagozzi, R. P. (2000) On the nature and direction of relationships between constructs and measures, *Psychological Methods*, 5, 155-174.
9. Fishbein, M., and Ajzen, I. (1975) Belief, attitude, intention and behavior: An introduction to theory and research.
10. Gefen, D., and Straub, D. (2005) A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example, *Communications of the Association for Information Systems (Volume 16, 2005)*, 91, 109, 109.
11. Hartwick, J., and Barki, H. (1994) Explaining the role of user participation in information system use, *Management Science*, 40, 4, 440–465.
12. Herath, T., and Rao, H. R. (2009) Protection motivation and deterrence: a framework for security policy compliance in organisations, *European Journal of Information Systems*, 18, 2, 106–125.
13. Hirschman, E. C., and Holbrook, M. B. (1982) Hedonic consumption: emerging concepts, methods and propositions, *The Journal of Marketing*, 46, 3, 92–101.
14. Hoadley, C.M., Xu, H., Lee, J.J., and Rosson, M.B. (2010) Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry, *Electronic Commerce Research and Applications*, 9,1, 50-60.
15. Johnston, A., and Warkentin, M. (2010) Fear Appeals and Information Security Behaviors: An Empirical Study, *MIS Quarterly*, 34, 1.
16. Kane, G. C., and Fichman, R. G. (2009) The Shoemaker's Children: Using Wikis for Information Systems Teaching, Research, and Publication, *MIS Quarterly*, 33, 1, 1–17.
17. Kankanhalli, A., Tan, B. C. Y., and Wei, K. K. (2005) Contributing knowledge to electronic repositories: an empirical investigation, *Management Information Systems Quarterly*, 29, 1, 7.
18. Ma, M., and Agarwal, R. (2007) Through a glass darkly: Information technology design, identity verification, and knowledge contribution in online communities, *Information Systems Research*, 18, 1, 42.
19. Moore, G. C., and Benbasat, I. (1991) Development of an instrument to measure the perceptions of adopting an information technology innovation, *Information systems research*, 2, 3, 192–222.
20. Nunnally, J. C., and Bernstein, I. H. (1978) Psychometric theory.
21. Ringle, C. M., Wende, S., and Will, A. (2005) SmartPLS 2.0, *Hamburg: University of Hamburg*.
22. Rippetoe, P. A., and Rogers, R. W. (1987) Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat, *Journal of Personality and social Psychology*, 52, 3, 596–604.
23. Rogers, R. W. (1975) A protection motivation theory of fear appeals and attitude change, *Journal of psychology*, 91, 1, 93–114.
24. Rogers, R. W. (1983) Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation, *Social psychophysiology*, 153–176.
25. Rogers, R. W., and Prentice-Dunn, S. (1997) Protection motivation theory, *Handbook of health behavior research*, 1, 113–132.
26. Stafford, T. F., and Poston, R. (2010) Online Security Threats and Computer User Intentions, *Computer*, 43, 1, 58–64.
27. Straub, D., Boudreau, M. C., and Gefen, D. (2004) Validation guidelines for IS positivist research, *Communications of the Association for Information Systems*, 13, 24, 380–427.
28. Straub, D. W. (1989) Validating instruments in MIS research, *MIS quarterly*, 13, 2, 147–169.
29. Venkatesh, V., and Davis, F. D. (2000) A theoretical extension of the technology acceptance model: Four longitudinal field studies, *Management Science*, 46, 2, 186–204.

30. Venkatesh, V., M. G. Morris, G. B. Davis, and F. D. Davis (2003) User Acceptance of Information Technology: Toward a Unified View, *MIS Quarterly*, 27, 3, 425-478.
31. Wasko, M., and Faraj, S. (2005) Why should I share? Examining social capital and knowledge contribution in electronic networks of practice, *Management Information Systems Quarterly*, 29, 1, 4.
32. Woon, I. M. Y., Tan, G. W., and Low, R. T. (2005) A protection motivation theory approach to home wireless security, in: *Proceedings of the Twenty-Sixth International Conference on Information Systems, Las Vegas*, 367–380.

APPENDIX A – SURVEY INSTRUMENT

Construct	Code	Item
Realized Threat	RTH-1	I have posted information to online social media websites that was used by others in a way which I did not approve.
	RTH-2	Some information I posted to online social media websites resulted in negative consequences for me.
	RTH-3	Information that I have shared on social media websites was used to unfairly make decisions or judgments about me.
Severity	SEV-1	If information I post to online social media websites were misused it could be damaging.
	SEV-2	If someone misused the information I post on online social media websites there could be serious consequences for me.
	SEV-3	If information I share on online social media websites was misused it would bother me.
Vulnerability	VUL-1	Information I post on social media websites could be made available to unknown individuals and entities without my knowledge.
	VUL-2	I feel I am vulnerable to misuse of the personal information I post to social media websites.
	VUL-3	It is possible that personal information I share on social media websites will be used in a way which I would not approve.
Rewards	REW-1	I enjoy posting information on social media websites.
	REW-2	Staying connected with others is easier because I share information on social media websites.
	REW-3	Sharing information on social media websites is fun.
	REW-4	Sharing information on social media websites makes me feel like I am part of one or more groups.
Perceived Threat (Index calculated based on standardized scores of these three items)	PT1	I believe sharing information on online social media websites could have negative consequences.
	PT2	I feel my personal information that I post to social media websites could be misused.
	PT3	I feel good when others that I know enjoy the information that I share on social media websites.
Social Influence	SI-1	People who are important to me think I should share information on social media websites.
	SI-2	My friends expect me to post information to social media websites.
	SI-3	People who's opinion I care about like it when I share information on social media websites.
	SI-4	In general, others encourage me to share information on social media websites.
Behavioral Intent	INT-1	I intend to share information about me on social media websites in the future.
	INT-2	I anticipate that I will post information about me on social media websites in the future.
	INT-3	I plan to share information about me on social media websites in the future.