Proceedings of the Eleventh International Symposium on
Human Aspects of Information Security & Assurance (HAISA 2017)

Factors Influencing the Use of Privacy Settings in Location-Based Social Networks

H. Oladimeji and J. Ophoff

Dept. of Information Systems, University of Cape Town, Cape Town, South Africa
e-mail: OLDHEN003@myuct.ac.za; jacques.ophoff@uct.ac.za

Abstract

In location-based social networks (LBSN) users provide location information on public profiles that can potentially be used in harmful ways. LBSNs have privacy settings that allow users to control the privacy level of their profile, thus limiting access to location information by others, but for various reasons users seldom make use of these privacy settings. Using Protection Motivation Theory (PMT) as a theoretical lens, this paper examines whether users can be encouraged to use LBSN privacy settings through fear appeals. Fear appeals have been used in various studies to arouse fear in users, to stop or reduce a risky behaviour through the threat of impending danger. However, within the context of social networking, it is not yet clear how fear-inducing arguments will ultimately influence the use of privacy settings by users. The purpose of this study is to investigate the influence of fear appeals on user compliance with recommendations to use privacy settings. A sample of LBSN users (n=248) completed a survey measuring the variables conceptualized by PMT. Analysis of the responses show that PMT provides promising explanation for the intention to use privacy settings by social network users.

Keywords

Location Based Social Networks, Protection Motivation Theory, Fear Appeal

1. Introduction

Despite the risks involved in the use of social-networking sites, most users do not seem to alter their sharing behaviour or change their privacy settings (Shin et al., 2012). Moreover, users engage in activities that jeopardize their online safety and reputation, such as posting location information that could be misused by online predators (Rainie et al., 2013). Incidents such as stalking, cyberbullying, sexual harassment and other forms of privacy threats continue to increase. Research shows that most of the previous incidents are due to carelessness and risky behaviour performed by the victims themselves (Ybarra & Mitchell, 2004). LBSNs allow users to track the movement and actions of friends and other users in the same social graph, and allow themselves to be tracked. With motives of being 'cool' and meeting new friends around, using privacy settings may not be an attractive option regardless of the possible dangers (Tufekci, 2008).

Due to reasons such as laziness and limited understanding of privacy settings some users tend to keep their default settings (Tschersich & Botha, 2014). Some users are simply uninformed about online threats to their privacy and the actions they can take

to protect themselves (Paine et al., 2007; Christofides et al., 2012). The most secure option for social-network users is to make use of the privacy settings on these services to prevent any form of privacy threats (Tschersich & Botha, 2014). According to Christofides et al. (2012), understanding the use of privacy settings on social-networking sites is critical, as many individuals fail to protect their location privacy securely.

Previous studies have recommended the use of persuasion in security management, specifically citing emotions as a leverage point from which persuasive messages can "affect attitudes and motivation in a positive manner" (Siponen, 2000, p. 12). This study investigates the influence of fear appeals in motivating users to use privacy settings to ensure their privacy and prevent future threats in LBSNs. A fear appeal is a persuasive message which contains elements of threat and then describes a suggested form of protective action (Johnson & Warkentin, 2010). It has been used in several studies to steer individuals away from risky behaviour (e.g. Johnson & Warkentin, 2010; Marett et al., 2011).

To examine the influence of fear appeals on the intention to use privacy settings, this study adopts PMT (Rogers, 1983), a theory developed in the field of health communication. It has been shown that PMT can explain individual behaviour and provide a more holistic understanding of why people perform these behaviours (Hanisch et al., 1998). The research question that will guide this study is: *How do fear appeals modify end-user behavioural intentions to use privacy settings in location-based social networks?*

The remainder of this paper is structured as follows. First a review of relevant literature on PMT leads to the development of our research hypotheses. Next the research methodology is briefly explained. Data analysis and a discussion of the results follow. Lastly a summary of the results and ideas for future work are given.

2. Background

To encourage security compliance researchers have used a range of theories, such as the general deterrence theory (GDT), rational choice theory (RCT), accountability theory, reactance and justice theories, and PMT. Recent studies on compliance resulting from threats, or fear, represent a shift from earlier GDT-based approaches to a stronger emphasis on PMT (Crossler et al., 2013). A key reason for this shift is that GDT and RCT are based on a foundation of command and control, whereas PMT is based on the idea of using persuasive messages, called 'fear appeals', which warn of a personal threat and describe countervailing measures that consist of protective behaviour (Floyd et al., 2000).

2.1. Fear Appeals

For decades, psychologists have studied why people respond or fail to respond to a message contained in a fear appeal (Witte, 1992). A fear appeal is "a persuasive message with the intent to motivate individuals to comply with a recommended

course of action through the arousal of fear associated with a threat" (Johnson & Warkentin, 2010, p.550). Research shows that fear appeals impact users' behavioural intentions to comply with recommended security action, but the impact varies among individuals (Herath & Rao, 2009; Marett, 2010; Rogers, 1983).

According to Witte (1992), a fear appeal is divided into two parts: the first contains statements designed to increase the degree of harm associated with a risk and the probability of the risk happening. The second part tries to increase the perceived efficacy related with a recommended response by providing easy steps to prevent the risk and emphasizing the importance of the recommended response in averting the risk. In situations where a fear appeal successfully prompts a significant perception of threat, an evaluation of the efficacy of the response (response efficacy) and one's ability to enact the response (self-efficacy) immediately follows.

2.2. PMT in Information Security Research

According to Boss et al. (2015), PMT is naturally suited for information security contexts in which end users and consumers require additional motivation to protect their information. Several information security studies use PMT as the primary basis for theory development (e.g. Herath & Rao, 2009; Lee & Larsen, 2009; Johnson & Warkentin, 2010). These studies include computer users' decisions to make use of antiviruses for their protection, employees' compliance with work-security policies, password protection and many more.

Studies show that some of the same factors that influence an individual's response to health and environmental risks could influence his response to technology-related risks (Marett, 2011). These factors include response costs, efficacy, risk severity and risk susceptibility. Although these studies were mainly focused on the intentions of individuals to adjust their behaviours in the face of security threats (Liang & Xue, 2009; Siponen et al., 2010), few studies have associated PMT with the intention to use privacy settings in LBSNs.

3. Hypothesis Development

Based on the body of literature around PMT the following hypotheses are formulated. Past research shows that perceived risk severity positively influences the security practices of individuals. For example, a study found that perceived severity positively affected whether people properly secured their wireless networks (Woon et al., 2005). Marett et al. (2015) also suggest that the perceived severity of a threat will have a positive influence on an individual intention to engage in the recommended action described in a fear appeal. Consistent with these studies it is proposed that: *H1: Perceived risk severity will positively influence the use of LBSN privacy settings.*

Risk susceptibility is the degree to which an individual believes the threat applies to his or her specific circumstances or the probability that the described threat will occur (Rogers, 1983). Perceived risk-susceptibility is regularly hypothesized to have

a positive relationship with security practices. However, findings are inconsistent in how perceived risk susceptibility affects these practices. For example, when explaining whether people will comply with security policies, perceived vulnerability did not have a significant relationship with security attitudes (Herath & Rao, 2009). A further study did not find a significant relationship between perceived susceptibility and properly securing wireless networks (Woon et al., 2005). Given the theoretical support from PMT, despite the mixed findings from prior research, it is proposed that: *H2: Perceived risk susceptibility will positively influence the use of LBSN privacy settings.*

Fear, a negative emotional response, results from perceived risk and perceived susceptibility. Therefore, risk severity and risk susceptibility predict fear (Floyd et al., 2000; Rogers & Prentice-Dunn, 1997), which acts as a partial mediator in the research model: *H3: Perceived risk severity will positively influence perceived fear. H4. Perceived risk susceptibility will positively influence perceived fear.*

Invoking fear can lead a person to take protective instructions more seriously (e.g. Rogers, 1983; Witte et al., 1992). Hence: *H5: An increase in fear will positively influence the use of LBSN privacy settings.*

Research shows that benefits derived from a risky behaviour did not have a positive influence on an adaptive response (Floyd et al., 2000; Leary & Jones, 1993). The results show that the perceived benefit increases the likelihood that some individuals will continue the risky behaviour rather than adopt a more protective behaviour. Marett et al. (2011) claims that the enjoyment gained from risky behaviours may simply be of stronger value for users than the perceived risk. Some LBSN users may have noted the potential danger caused by revealing their location information online, but perhaps the enjoyment from being able to display their location information is believed to be worth the risk, hence: *H6: Perceived sharing benefits will negatively influence the use of LBSN privacy settings.*

Self-efficacy refers to the belief in one's ability and willpower to make the recommended behavioural change to produce outcome (Bandura, 1977). According to Marrett et al. (2011) users' self-efficacy positively influenced an adaptive response. Further studies found a positive relationship between self-efficacy and the use of antispyware software (Johnston & Warkentin, 2010) as well as properly securing a home wireless network (Woon et al., 2005) and complying with security policies (Herath & Rao, 2009). It is proposed that: *H7: Perceived self-efficacy will positively influence the use of LBSN privacy settings.*

PMT posits that as the response cost goes up, the likelihood of performing the adaptive coping response goes down. For example, research supports these findings with response cost negatively influencing whether people properly secure their home wireless network (Woon et al., 2005). Other studies revealed that response costs (efforts) negatively influenced adaptive responses (Leary & Jones, 1993; Marett et al., 2011). Findings from previous research suggest that as the cost of invoking a coping response increases, then the likelihood of implementing the response goes

down, hence: *H8: Perceived response cost will negatively influence the use of LBSN privacy settings.*

Response efficacy or outcome expectations as it is regularly used in studies to represent a "person's estimate that a given behaviour will lead to certain outcomes" (Bandura, 1977). Response efficacy was shown to positively influence adaptive behavioural response; users who believed the suggested behavioural change would be effective against threats were more likely to engage in adaptive behaviours (Marett et al., 2011). It is proposed that: *H9: Perceived response efficacy will positively influence the use of LBSN privacy settings.*

A maladaptive behaviour is any kind of behaviour that prevents individuals from protecting themselves. It could be avoidance or hopelessness (Floyd et al., 2000; Rogers & Prentice-Dunn, 1997). Avoidance involves a defensive resistance to information advising an individual on how to reduce the risk associated with a behaviour (Marett et al., 2011). Hopelessness refers to a belief that a threat is unavoidable no matter what is done by an individual (Rippetoe & Rogers, 1987). It is proposed that: *H10a. Maladaptive avoidance behaviour will negatively influence the use of LBSN privacy settings. H10b. Maladaptive hopelessness behaviour will negatively influence the use of LBSN privacy settings.*

4. Research Methodology

A web-based survey (hosted on Qualtrics) using a questionnaire was used to collect data about users' perceptions and behaviours in a systematic way. The survey contained demographic questions and variables from the conceptual model, based on previous instruments (Marett et al., 2011; Johnson & Warkentin, 2010; Woon et al., 2005; Osman et al., 1994; Milne et al., 2000; Myyry et al., 2009). The measurement items used a 5-point Likert scale.

A fear appeal was issued to the participants prior to answering the questions. The fear appeal was adapted from studies by Marett et al. (2011) and Johnston & Warkentin (2010). A series of questions were asked to measure the impact of the fear appeal on the intention to use privacy settings in LBSNs. The survey was distributed via email to a random sample of students at a large research university. The sample is similar to previous studies in this domain (e.g. Johnson & Warkentin, 2010).

To ensure the dataset was free of errors a data-cleaning process was performed in which incomplete and unengaged responses were removed. Analysis of the cleaned data was done using Partial Least Square Structural Equation Modelling (PLS-SEM). PLS-SEM is "an ordinary least squares (OLS) regression-based method which uses available data to estimate the path relationships in the model" (Hair et al., 2013, p. 14). The approach is suitable for validating predictive models. The SmartPLS 3 software was used.

5. Data Analysis

A total of 446 responses were collected. From these 198 incomplete responses were removed, leaving a final dataset of 248 responses which were used for data analysis. There were 133 responses in which no questions were answered, which could be due to a reluctance to read the fear appeal and no incentives were offered. The demographic data indicates a young (70.2 percent younger than 25) and predominantly female (60.1 percent) sample, with relatively good experience of LBSNs (69.4 percent with more than 3 years' experience). The systematic procedure suggested by Hair et al. (2016) was followed for analysis, which started with estimating the path model and assessing the reflective measurement model.

5.1. Analysis of the Measurement Model

The research model was developed as a reflective measurement model. A model is said to be reflective if the indicators are highly correlated and interchangeable (Hair et al., 2013). Due to the high correlations their reliability and validity should be thoroughly examined. Regarding internal consistency reliability all variables were above the recommended composite reliability threshold (0.70). In terms of convergent validity two indicators with weak outer loadings (<0.40) were removed. The remaining indicators' reliability was acceptable. The average variance extracted (AVE) for variables were above the recommended threshold (0.50), except Maladaptive Avoidance (0.49) which was deemed acceptable. Finally, discriminant validity was measured using the heterotrait-monotrait (HTMT) ratio of correlations, which showed that all variables were below the 0.90 threshold. All model evaluation criteria were met, providing support for the measures' reliability and validity.

5.2. Analysis of the Structural Model

The structural model was tested to estimate the path coefficients, which calculates the strength of the relationships between variables. The coefficients of determination (R^2) values were estimated to determine the variance explained by the independent variables. These showed an effect size of 0.372 for the use of privacy settings endogenous latent variable, as well as 0.415 for fear. compared to previous studies in information security with similar variables, the values show a medium to high effect size (Boss et al., 2015). In addition, the f^2 effect size showed a medium effect (0.160) of Risk Susceptibility on Fear.

Bootstrapping with 5,000 samples (recommended by Hair et al., 2016) was used to test the significance of the structural paths (hypotheses). The bootstrapping results show that only H1, H5, and H8 are not significant. The PLS path modelling estimation, including path coefficients and p-values, is shown in Figure 1. The results of hypothesis testing are summarized in Table 1.

5.3. Discussion

Overall the model shows good fit to the problem domain. The significant relationships help to expand knowledge about how fear appeals operate. Considering the hypotheses that were not supported, response cost bordered on a statistically significant value (p=0.053) which suggests that this is a concern for the use of privacy settings. The level of cost/inconvenience may vary across social networks.

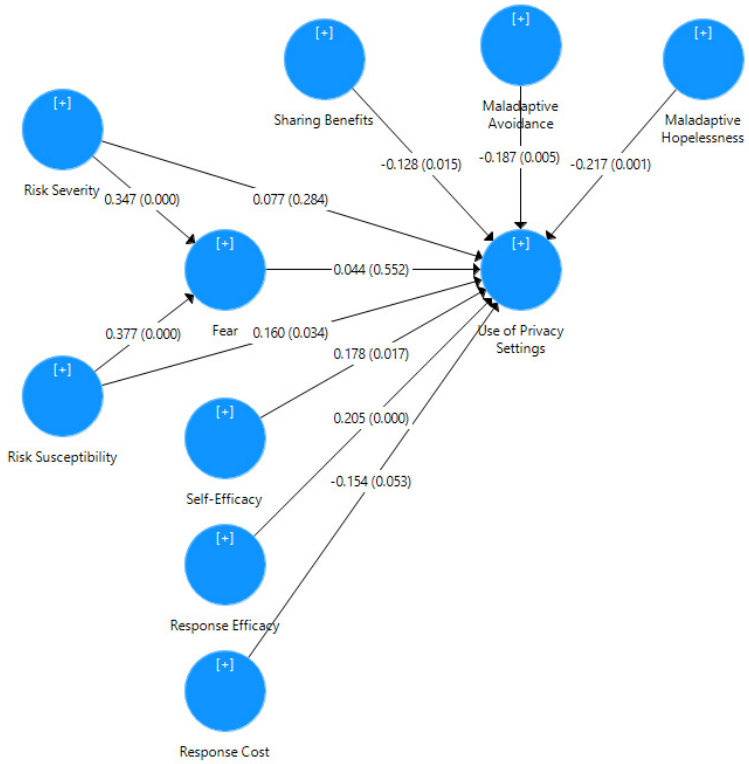

Figure 1: Structural Model Analysis

Hypothesis	Path Coefficient	T Value	P Value	Supported?
H1	0.077	1.071	p > 0.10	Not supported
H2	0.16	2.125	p < 0.05	Supported
H3	0.347	5.042	p < 0.001	Supported
H4	0.377	5.717	p < 0.001	Supported
H5	0.044	0.594	p > 0.10	Not supported
H6	-0.128	2.442	p < 0.05	Supported
H7	0.178	2.383	p < 0.05	Supported
H8	-0.154	1.933	p > 0.05	Not supported
H9	0.205	4.069	p < 0.001	Supported
H10a	-0.187	2.791	p < 0.01	Supported
H10b	-0.217	3.185	p < 0.01	Supported

Table 1: Overview of Findings

The influence of perceived risk severity on the use of privacy settings was not significant. This is not a surprising result as previous studies have found that perceived risk severity is insignificant on the decision to change risky behaviour (e.g. Liang & Xue, 2009; Lee & Larsen, 2009). This is also supported in health science studies (e.g. Milne et al., 2000). The tendency to underestimate one's chance of becoming a victim may be one of the obstacles hindering people from adopting precautionary behaviours (Marett et al., 2011). It is also important to acknowledge that the insignificant e□ect may stem from the fact that the fear appeal wasn't strong enough to make users perceive the seriousness of online threat (Boss et al., 2015).

The influence of fear was not significant, and it did not play a role in mediating the impact of susceptibility and severity on intention. This result is consistent with PMT, which identifies fear as a by-product of the message but not an integral part of the persuasion model (Rogers, 1983). Even though individuals, who were made to feel susceptible, perceived the privacy risk as more threatening and experienced more fear, it was the threat perception and coping appraisal rather than the effect of fear that appeared to have motivated them to engage in the recommendation.

6. Conclusion

While numerous studies have pointed to the use of emotional messages to inspire end users to practice online safety, few studies have conceptualized and tested a model for understanding how users will respond to fear-inducing messages in LBSNs. This study theoretically validates PMT in this context and provides administrators with insight for tailoring fear appeals for maximum effect. For example, response efficacy emerged as a significant determinant of intention to use privacy settings. Therefore, focusing more on the coping appraisal, rather than threat appraisal, when designing fear appeals could improve effectiveness.

Current applications of PMT effectively explain the processes and outcomes of danger control, but they have been mostly silent on the processes and outcomes of fear control (Boss et al., 2015). Future research should explore the possible dual outcomes by considering the dual-process routes afforded by the dual-process model (Leventhal, 1970) or by the more recent extended parallel process model (Witte, 1992).

7. References

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological Review*, 84(2), 191.

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

Christofides, E., Muise, A., & Desmarais, S. (2012). Risky disclosures on Facebook: The effect of having a bad experience on online behavior. *Journal of Adolescent Research*, 27(6), 714-731.

Crossler, R., Johnston, A., Lowry, P., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32, 90-101.

Floyd, D., & Prentice-Dunn, S., and Rogers, R. (2000). A Meta-analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, 30 (2), 407-429.

Hair, J., Ringle, C., & Sarstedt, M. (2013). Editorial-partial least squares structural equation modeling: Rigorous applications, better results and higher acceptance. *Long Range Planning*, 46(1-2), 1-12.

Hair, J., Hult, G., Ringle, C., & Sarstedt, M. (2016). *A Primer on Partial Least Squares Structural Equation Modeling 2e*. Los Angeles: SAGE Publications.

Hanisch, K., Hulin, C., & Roznowski, M. (1998). The importance of individuals' repertoires of behaviors: The scientific appropriateness of studying multiple behaviors and general attitudes. *Journal of Organizational Behavior*, 19(5), 463-480.

Herath, T., & Rao, H. (2009). Protection motivation and deterrence: a framework for security policy compliance in organizations. *European Journal of Information Systems*, 18(2), 106-125.

Johnston, A., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviours: An Empirical Study. *MIS Quarterly*, 34(3), 549-566.

Leary, M., & Jones, J. (1993). The Social Psychology of Tanning and Sunscreen Use: Self-presentational Motives as a Predictor of Health Risk. *Journal of Applied Social Psychology*, 23(17), 1390-1406.

Lee, Y., & Larsen, K. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, 18(2), 177-187.

Leventhal, H. (1970). Findings and theory in the study of fear communications. *Advances in Experimental Social Psychology*, 5, 119-186.

Liang, H., & Y. Xue. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly*, 33(1), 71-90.

Marett, K., McNab, A., & Harris, R. (2011). Social networking websites and posting personal information: An evaluation of protection motivation theory. *AIS Transactions on Human-Computer Interaction*, 3(3), 170-188.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and Intervention in Health-related Behaviour: A Meta-Analytic Review of Protection Motivation Theory. *Journal of Applied Social Psychology*, 30(1), 106-143.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, 18(2), 126-139.

Osman, A., Barrios, F., Osman, J., Schneekloth, R., & Troutman, J. (1994). The Pain Anxiety Symptoms Scale: psychometric properties in a community sample. *Journal of Behavioral Medicine*, 17(5), 511-522.

Paine, C., Reips, U., Stieger, S., Joinson, J. & Buchanan, J. (2007). Internet Users' Perceptions of 'Privacy Concerns' and 'Privacy Actions'. *International Journal of Human-Computer Studies*, 65(6) 526-536.

Rainie, L., Smith, A., & Duggan, M. (2013). *Coming and going on Facebook*. Pew Research Center's Internet and American Life Project.

Rippetoe, P., & Rogers, R. (1987). Effects of Components of Protection-motivation Theory on Adaptive and Maladaptive Coping with a Health Threat. *Journal of Personality & Social Psychology*, 52(3), 596-604.

Rogers, R. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social Psychophysiology*, 153-176.

Rogers, R., & Prentice-Dunn, S. (1997). *Protection Motivation Theory*, in D. Gochman (Ed.) Handbook of Health Behaviour Research I. New York, NY: Plenum.

Shin, K., Ju, X., Chen, Z., & Hu, X. (2012). Privacy protection for users of location-based services. *IEEE Wireless Communications*, 19(1).

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), 31-41.

Siponen, M., Pahnila, S., & Mahmood, M. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer*, 43(2), 64-71.

Tschersich, M., & Botha, R. (2014). Exploring the impact of restrictive default privacy settings on the privacy calculus on social network sites. *In proceedings of the European Conference on Information Systems (ECIS)*, Tel Aviv, Israel.

Tufekci, Z. (2008). Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology, and Society*, 28(1), 20-36.

Witte, K. (1992). Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model. *Communication Monographs*, 59(4), 329-349.

Woon, I., Tan, G., & Low, R. (2005). A protection motivation theory approach to home wireless security. *In proceedings of the International Conference on Information Systems (ICIS)*, 31.

Ybarra, M., & Mitchell, K. (2004). Online aggressor/targets, aggressors, and targets: A comparison of associated youth characteristics. *Journal of Child Psychology and Psychiatry*, 45(7), 1308-1316.