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

A DISSERTATION PRESENTED TO THE

DEPARTMENT OF INFORMATION SYSTEMS

UNIVERSITY OF CAPE TOWN

BY

HENRY OLADIMEJI

Supervised by: Dr Jacques Ophoff

March 2017

In partial fulfilment of the requirements for the Masters of Commerce in Information Systems

DECLARATION

I, Henry, Oladimeji, hereby declare that the work on which this thesis is based is my original work (except where acknowledgements indicate otherwise) and that neither the whole work nor any part of it has been, is being, or is to be submitted for another degree in this or any other university. I authorise the University to reproduce for the purpose of research either the whole or any portion of the contents in any manner whatsoever.

Signature: Signed by candidate
Signature Removed

Date: 16 /03 /2017

ABSTRACT

The growth of location-based social networks (LBSN) such as Facebook and Twitter has been rapid in recent years. In LBSNs, users provide location information on public profiles that potentially can be used in harmful ways. LBSNs have privacy settings that allow users to control the privacy level of their profiles, thus limiting access to location information by other users; but for various reasons users seldom make use of them.

Using the protection motivation theory (PMT) as a theoretical lens, this dissertation 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, in order to motivate them to comply to an adaptive 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 enact the use of privacy settings toward the alleviation of privacy threats.

Using a survey methodology, 248 social-network users completed an instrument measuring the variables conceptualized by PMT. Partial Least Squares Structural Equation Modelling (PLS-SEM) was used to test the validity and reliability, and to analyze the data. Analysis of the responses show that PMT provides an explanation for the intention to use privacy settings by social-network users. Risk susceptibility, response efficacy, self-efficacy and response cost were found to have a positive impact on the intention to use privacy settings, while benefits and maladaptive behaviours were found to have a negative impact on the intention to use privacy settings. However, risk severity and fear were found to be insignificant predictors of the intention to use privacy settings.

This study contributes to existing research on PMT in a sense that fear appeal should focus more on coping appraisal, rather than on threat appraisal which is consistent with the results of most studies on protection motivation.

ACKNOWLEDGEMENT

I give my utmost gratitude to my supervisor Dr Jacques Ophoff for his unwavering support, encouragement, constructive critiques, guidance, and distinguished teaching all through the journey to the completion of this research.

My deepest gratitude I give to Banji Oluwole, Juliet Oladimeji, Toyin Abolumo, Gbemisola Afolabi and Deborah Ajumobi for being there from the start of this journey, even at times when I could not be there for myself, and for supporting me with their love and prayers.

I would also like to thank my colleagues in the IS Department for their encouragement and academic mentorship, and the students of the University of Cape Town who participated in this research.

DEDICATION

I dedicate this dissertation to God Almighty. His grace has been sufficient thus far. I would also like to dedicate this dissertation to my parents, my brothers and my sisters – I am very grateful for your endless love and support.

Table of contents

1 INTRODUCTION

1.1 Background

The growth of Social Networking Sites (SNS) has been rapid in recent years, and this has made communication easier and better. SNS are web-based services that allow individuals to: construct a public or semi-public profile; articulate a list of other users; view and negotiate their list of connections and those made by others within the system with the aim of communicating and maintaining relationships (Borena, Belanger & Ejigu, 2013). Kaplan and Haenlein (2010) describe SNSs as applications that enable users to connect with each other by creating personal information profiles, inviting friends, family and colleagues to have access to those profiles, and sending e-mails and instant messages between each other. These personal profiles can include any type of information, including photos, videos, audio files, and location (Kaplan & Haenlein, 2010). Approximately 50 percent of active social networking site users log on to their profile daily and over 30 billion pieces of content are shared on social networking sites monthly (Facebook, 2014).

SNS users can share photos, personal information, location information, and news about themselves in a shared space that can be made accessible to others in varying degrees (Saeri, Ogilvie, La Macchia, Smith & Louis, 2014). With this amount of content being shared, the impact of what is posted and the use of privacy settings to control access is important. During the use of SNS, people are confronted with information-privacy concerns and consequently privacy-protection behaviour. Privacy can be understood as the ''boundary control process in which individuals regulate when, how and to what extent information about them is communicated to others'' (Garde-Perik, Markopoulos, Ruyter, Eggen & Wijnand Ijsselsteijn, 2008, p. 21).

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) and very few take action to protect their privacy (Comparatives, 2013; Cyber Security, 2012). Moreover, they engage in activities that jeopardize their online safety and reputation, such as posting location information that could be misused by online predators (Microsoft, 2014; Rainie et al., 2013).

1.2 Information Sharing Risks

The media and shared experiences by victims have shown that these networks are prime targets for online predators and troublemakers. According to the 2013 Computer Crime and Security Survey, 46 percent of social-network users reported some form of privacy issues during the past year (Maximilien et al., 2009). Moreover, incidents such as stalking, cyberbullying, sexual harassment and other forms of privacy threats continue to increase, with the average reported incidents by users increasing by 10 percent from 2011 to 2013 (Richardson, 2013). These figures most likely understate the level of the problem facing users, since research shows that some victims are too scared or ashamed to report some incidents (Hoffer & Straub, 1989).

Research shows that most of the previous incidents are due to carelessness and risky behaviour performed by the victims themselves (Ybarra & Mitchell, 2004). SNS are particularly attractive to young adults, with more than half of users being in the 18 to 34-year age-range (Goldinsidenetwork, 2011). This age group generally is made up of individuals who are just starting or further establishing their professional lives, whether in a university setting or in the workplace, and are developing their professional identities. According to the study, these age group pays less attention to privacy. The result of the survey showed that 69 percent of individuals included their physical location in a social networking status update, and 24 percent of them are friends with strangers (McAfee, 2010). Criddle (2006) advised social-network users to refrain from making their personal information, especially their location information, public without serious consideration of the risks. Another survey shows that 46 percent of Facebook users willingly make location information and other personal information public, making them susceptible to privacy threats (Sophos Labs, 2011).

According to Lampe et al. (2010), LBSN like Facebook allow users to track the movement and actions of friends and other users in the same social graph, and allow themselves to be tracked. The surveillance and 'social search' functions of these networks may explain why so many users leave their privacy settings relatively open. Gross and Acquisti (2011) report that only 1.2 percent of users changed the default 'search' privacy setting, and less than 50 percent of users changed the default 'profile visibility' privacy settings.

This enables other users who are not currently linked as friends to view location information and other personal information. To some users, it is a means of increasing the size of their social network and meeting people of similar interests nearby. The rewards derived from

posting location information, and socializing with friends doing likewise, apparently outweigh the potential danger for some social-network users. 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).

1.3 Encouraging use of Privacy Settings

Research also shows that due to some reasons, including laziness and limited understanding of privacy settings, some users tend to keep their default settings (Tschersich et al., 2014). Some users are simply uninformed about online threats to their privacy and to 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 et al., 2014).

According to Christofides, Muise and Desmarais (2012), understanding the use of privacy settings on social-networking sites is critical, as many individuals fail to protect their location privacy securely. Perhaps users can be nudged to use privacy settings through fear appeals. Fear appeals have been used in previous research to persuade a healthy behaviour and prevent harm. For network providers desiring the use of privacy settings by LBSN users, the use of persuasive communications may be especially appealing (Markett, 2010).

Scholars 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). Persuasive arguments can be embedded in various artifacts to which users are exposed (O'Keefe, 1990; Rogers et al., 1983). 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. Fear appeal is a persuasive message which contains elements of threat, which include the susceptibility and severity of the 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 (Johnson & Warkentin, 2010; Markett et al., 2011; Johnson, 2015; Hoog et al., 2005). The purpose of a fear appeal is to effect change through persuasion (Roskos-Ewoldsen et al., 2004).

Researchers and professionals agree that people are often the weakest link in security (Crossler et al., 2013), but until recently, few studies have tried to understand the human

component of a secure information system (Cannoy et al., 2006; Choobineh et al., 2007; Dhillon & Backhouse, 2001). A number of theories have been explored to explain security behaviour, including the theory of planned behaviour (e.g. Dinev & Hu, 2007), the general deterrence theory (e.g. Herath & Rao, 2009b), and the protection motivation theory (e.g. Anderson & Agarwal, 2010; Johnston & Warkentin, 2010). Several of these studies have used an adaptation of the Protection Motivation Theory (PMT) to explain differences in security practices.

1.4 Research Question and Objective

Many studies have tested the PMT measuring intention to use a security tool like anti-spyware (e.g. Johnston & Warkentin, 2010; Kumar et al., 2008) intentions to generically perform security-related behaviour (e.g. Anderson & Agarwal, 2010), or intentions to comply with security policies (e.g. Herath & Rao, 2009b), but none has used PMT to study the intention to use location-privacy settings in social networking sites after being issued with a fear appeal. In order to examine the influence of fear appeal on the intention to use privacy settings, this study adopts PMT, a theoretical framework developed in the field of health communication. It has been shown that PMT can explain individual behaviour and also provide a more holistic understanding of why people perform these behaviours (Hanisch et al., 1998)

The following presents the objective and research question that will guide this study: *How do fear appeals modify end-user behavioural intentions associated with the use of privacy settings in location-based social networks?*

The objective is to understand the factors that influence the use of privacy settings toward the alleviation of privacy threats in using location-based social networking sites by users after being issued with a fear appeal.

1.5 Importance of research

This study contributes to information-security research by adapting and testing a model developed in the field of medical sciences in an IS domain to provide a better understanding of the factors that influence individual security behaviours.

The societal value of this study is to find out how fear appeal can be used to motivate the use of privacy settings by social networking-sites users. This will also help service providers with the design of fear appeal by focusing more on the factors that have positive influence on users to adopt protective behaviour, hence leading to more efficiency.

This paper contributes to research on computers and security by expanding the understanding of fear appeal and PMT by empirically testing these through the use of location-privacy settings in social networking sites and integrating commonly ignored PMT variables: maladaptive behaviour and benefits (Boss et al., 2015) into the PMT model to further examine the cognitive coping process related to an expression of intention to take security protective actions.

1.6 Dissertation overview

The rest of the dissertation is presented in the following order:

- **Chapter 2** comprises the review of literature on social networking sites, fear appeal, the Protection Motivation Theory and the variables proposed to impact on the intention to use privacy settings in location-based social networking sites. It also shows the gaps identified in the literature review and the conceptual model developed, based on the review done and the gaps identified. This conceptual model illustrates the relationship between the constructs and the proposed outcome. The last section outlines the hypotheses formulated and tested in the study.
- **Chapter 3** provides detail on the research design by discussing the philosophical stance taken; the research methodology which comprises of the research paradigm adopted; the research purpose; research approach; research strategy; the data collection and analysis method; and the ethics and confidentiality issues considered for the study.
- **Chapter 4** includes a presentation of results and findings from the data analysis carried out, as well as a discussion of these findings and results of the hypothesis testing.
- **Chapter 5** consists of the conclusion to the dissertation, which includes theoretical and practical implications, recommendations and suggestions for further research.

2 LITERATURE REVIEW

2.1 Privacy settings in LBSNs

Each LBSN has its own location privacy settings, and some are more complicated than others. Due to its popularity, a description of privacy settings on Facebook will be given as an example. Facebook is the most popular LBSN with over 1 billion active monthly users (Facebook, 2016). Facebook's privacy settings are extremely detailed, giving users the ability to fine-tune the privacy aspects of almost every part of their account. Privacy settings give users the opportunity to have control over the type of information shared and with whom they choose to share with. This information varies from birthdays, pictures, interests, political and religious views and status updates to location information such as current city and places the user checks into. Privacy settings for sharing information are separated from the settings for connecting with other users. Controlling what content to share and with whom is important. Facebook privacy settings let the users share content with everyone, friends of friends or friends only. It also allows the users to customize the settings and set a certain type of content to be visible to the people on some of the user's friend list and invisible to others. For example, only my close friends can see where I check into (location information) while my business associates cannot. Below are screengrabs of privacy settings on Facebook:

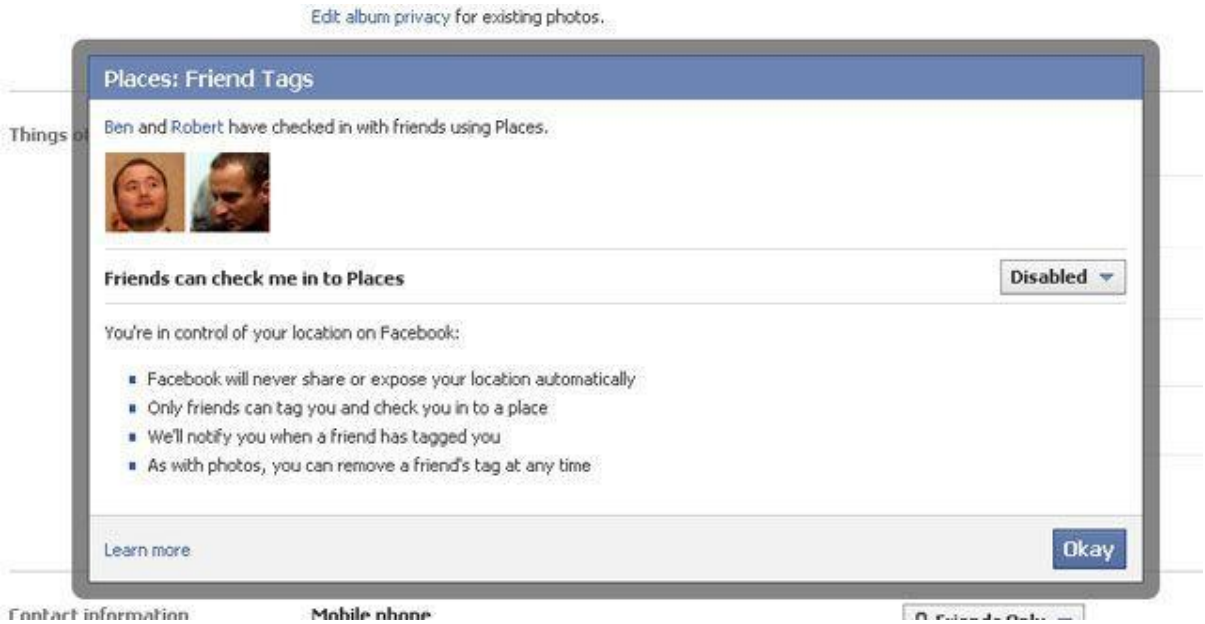


Figure 1: How to control location check in

The above location privacy setting lets friends check you into places. These feature on SNS allows someone else expose your location information to other SNS users. To prevent that from happening, the user can simply disable “friends can check me in to places”.

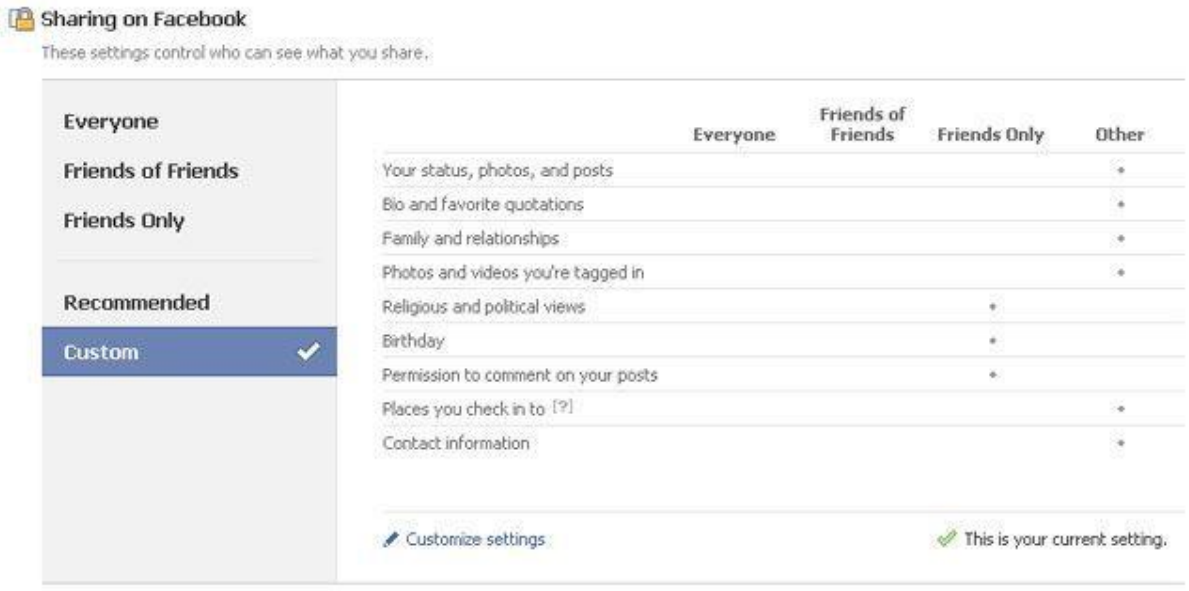


Figure 2: Settings that control who can see what the users share

The above privacy setting lets the user have control over with whom he wants to share his location information and other personal information. The user can decide to share his location information with everybody, friends of friends or friends only.

Figure 3: Showing how to enable or disable ‘check ins’

The above privacy setting lets users ‘check in’ to places. Once a user checks in to a place, his location information is made public for other users to see. To prevent this, the user can simply disable the ‘check in’ feature on his account.

The following section uses a suitable theory to motivate information security behavior.

2.2 Motivating Information Security Behaviour

Many recent information-security studies have focused on finding ways to motivate home users and employees to improve the protection of their individual and organizational information assets (Boss et al., 2015). To encourage security compliance, researchers have

used the different theories – such as the general deterrence theory (GDT; Herath & Rao, 2009; Hu et al., 2011), the rational choice theory (RCT; Bulgurcu et al., 2010; Hu et al., 2011), the accountability theory (Vance et al., 2013 and 2015), the reactance and justice theories (Lowry & Moody, 2015; Lowry et al., 2015; Posey et al., 2011; Wall et al., 2013), and the protection-motivation theory (PMT; Crossler & Bélanger, 2014; Herath & Rao, 2009; Lee & Larsen, 2009). 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).

2.3 Fear Appeals

Different approaches to fear appeals have been taken to persuade people to embrace certain intentions or actions. For decades, psychologists have studied why people respond or fail to respond to a message contained in a fear appeal (Witte, 1992). A simplified definition of 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, 2010, p.550). Research shows that fear appeals impact users' behavioural intentions to comply with recommended security action, but the impact varies among individuals (Johnson, 2015; Herath, 2009; Marett, 2010; Rogers, 1983). The components of fear appeal include threat severity, threat susceptibility, and self-efficacy and response efficacy (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. According to PMT, fear appeal is only useful when a threat is perceived to be relevant and potentially harmful. In other words, if an individual is exposed to a fear appeal that does not arouse a personally relevant perception of threat, then no further information processing occurs (Johnson & Warkentin, 2010). 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 (Johnson, 2015). In situations in which perceived threat is accompanied by a moderate-to-high degree of perceived efficacy, individuals will take action to mitigate the threat. A reasoning process whereby strategies are employed to avert a threat is followed. This process is one that can lead to positive outcomes; in this study it is proposed to be the use of privacy settings by LBSN users.

2.4 PMT in the Information Security Field

In order to examine the influence of fear appeals on the use of privacy settings, we adapt PMT, a theoretical framework used in the field of health communication. It was originally developed to explain the effects of fear appeals on health behaviour. PMT was adapted to examine the influence of fear appeal on the recipients' use of privacy settings in LBSNs.

According to the theory, the elements of fear appeal attribute to the way individuals would respond to a threat. The levels of these components determine the levels of an individual's protection motivation (Rogers, 1975 and 1983). PMT is a well-developed theoretical foundation for the analysis and exploration of recommended actions or behaviours to avert the consequences of threats (Johnson, 2010).

PMT has been widely used, primarily in the application of fear appeals directed toward threats and recommended action, e.g. the use of condoms to prevent the spread of STDs (Tanner et al., 1991), the use of sunscreen during sun tanning to prevent skin cancer (McMath & Prentice-Dunn, 2005); and smoking cessation to prevent cancer (Maddux & Rogers, 1983) among others. PMT has been used to explain the choices individuals make when deciding whether to continue to engage in the risky activity or to better protect themselves (Maddux, 1993). Research shows that while some individuals take precautions after being warned about threats, others choose to ignore the same information and continue with the risky behaviour. PMT has been infrequently applied to individuals' risky use of social networking and other technologies in general.

Recently some research in information systems adapted PMT, using the same health-related variables to help explain security awareness (Ng et al., 2009). 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 that use PMT as the primary basis for theory development have been published in information systems (IS) journals (e.g. Herath & Rao, 2009; Johnston & Warkentin, 2010a; Lee et al., 2008; Lee & Larsen, 2009; Liang & Xue, 2010; Pahnila et al., 2007). 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.

These 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.

PMT centers upon the act of making a fear appeal to individuals at risk from some danger in order to persuade them to change their behaviour (Rogers & Prentice-Dunn, 1997). A fear appeal does not just induce fear; it also includes a recommended response to a threat. In this study, the recommended response is the use of privacy settings in LBSNs. It is important to highlight that the feeling of fear is conceptually different from the fear appeal message. In the context of PMT, fear is defined as a "relational construct aroused in response to a situation that is judged as dangerous and towards which protective action is taken" (Rogers, 1975, p.96).

PMT proposes that protective behaviour is motivated by two processes, namely threat and coping appraisals (Floyd et al., 2000; Rogers, 1975). Upon receiving the fear appeal, a threat appraisal is done by the individual who involves assessment of the risk to their safety (McClendon & Prentice-Dunn, 2001). These appraisals are described as cognitive mediating processes that together lead to protection motivation, which in turn acts as a motive for choosing an adaptive behaviour. The cognitive mediating process is illustrated in Figure 4.

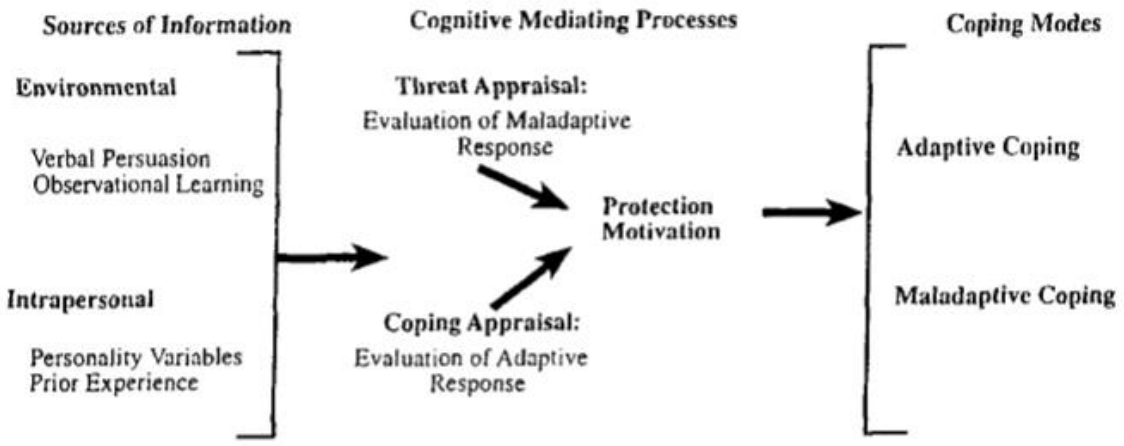


Figure 4: A Schematic Model of the Cognitive Processes Described by Protection Motivation Theory (adapted from Floyd et al., (2000)

Threat appraisal assesses the severity and susceptibility, while coping appraisal focuses on the possibilities to avert the threat or to cope with it (Floyd et al., 2000). As indicated earlier, the outcome of these appraisal processes is the formation of the decision to initiate, inhibit, or continue certain behaviour. In the context of this study, the result of these processes could either be an intention to use location privacy-settings or not.

2.4.1 **Threat appraisal**

This simply means an evaluation of how threatened one is in a certain situation. Fear appeals, which are the starting point for the threat appraisal, can be aroused by information acquired from previous experiences (Floyd et al., 2000). This information helps when evaluating the threat by the probability that it actualizes (susceptibility) and by the severity of the consequences if it occurs (severity) (Floyd et al., 2000; Rogers, 1975). Evaluations of susceptibility and severity lead to different levels of fear which motivate the selection of an adaptive response.

Threat appraisal is also affected by benefits associated with a certain type of behaviour. A user can perceive a certain security threat to be significant but not fear-evoking for himself. If this kind of evaluation is accompanied by the maladaptive behaviour of saving one's own time and effort by not engaging in secure behaviours, the unsecured behaviour is more likely. Avoidance and hopelessness are the two types of maladaptive behaviours (Rippetoe & Rogers, 1987). Avoidance in this context means a resistance to information advising the

individual on how to reduce the risk associated with the threat of interest (Witte, 1992). Hopelessness in this context is the belief that the threat is unavoidable no matter the action taken by the individual, this response most likely will result to the continuation of the risky behaviour (Rippetoe & Rogers, 1987).

2.4.2 Coping appraisal

This includes the assessment of the response efficacy and self-efficacy of possible coping methods in dealing with the threat. Response efficacy is the degree to which an individual believes that a recommended response will be effective in averting the threat, and self-efficacy is the belief that an individual can successfully implement the recommended response (Floyd et al., 2000; Maddux & Rogers, 1983). Positive evaluations of response efficacy and self-efficacy are likely to increase the probability of an adaptive response to the threat. Adaptive response is simply an intention to change a behaviour pattern to reduce or prevent the risk associated with the behaviour (Fry & Prentice-Dunn, 2005).

In addition to efficacy evaluations, response costs are assessed during the coping appraisal. Response cost is the time and effort required to carry out the recommended response (Floyd et al., 2000). If the costs of responding adaptively to the situation are high, the probability of adaptive behaviour is reduced. These evaluations can then either compensate the effects of threat appraisal process, lead to an adaptive response, or weaken the perceived ability to react adaptively to the threat. In general, threat and coping appraisal processes lead jointly to protection motivation and affect the selection of behaviours in a certain situation, for example the choice to make use of privacy settings.

2.4.3 Behavioural Intention

According to PMT, the outputs of the processes should predict the impact of the fear appeal, and these impacts are usually measured as behavioural intentions (Rogers & Prentice-Dunn, 1997). PMT demonstrates how the conflicting influences of the model constructs impact an individual's behavioural intentions to either continue with the risky behaviour or restrain from the risky behaviour (McMath & Prentice-Dunn, 2005). The purpose of the present study is to extend prior research on PMT into the field of LBSNs and information privacy. Privacy experts recommend that LBSN users make use of privacy settings to control access to location information disclosed on their profile. Thus the adaptive response in this study is the use of privacy settings.

PMT contends that the probability of an adaptive response increases through one's belief that the threat poses a substantial risk to the individual, that an adaptive response will be effective for improving protection (response efficacy), and that the individual has the ability and the confidence to make necessary changes (self-efficacy) (Rogers & Prentice-Dunn, 1997). Therefore, according to PMT, LBSN users who perceive the potential risk of posting location information as being high, or who believe in their ability to follow the recommended privacy settings, or who believe the recommended changes are capable of preventing their location information from being exploited are more likely to make the adaptive response. Likewise, other PMT variables, such as benefits and response costs will reduce the chance for an adaptive response (Marett et al., 2011). In other words, if a LBSN user highly enjoys the gratification he receives from posing location information, if he believes posting location information will influence his status or reputation within the network, or if the costs associated with removing location information throughout his profile are undesirably high, we expect the probability that the user will make use of the privacy settings will be reduced (Marett et al., 2011). The PMT variables can help explain a LBSN user's decision to use privacy settings.

2.5 PMT Findings in Information Security Research

Several studies have found support for the assumptions of PMT in the field of information security. Workman, Bommer and Straub (2008) noticed that perceived susceptibility and severity, as well as response efficacy and self-efficacy, explained both the subjective and objective behaviours of users as the theory assumes. However, there are also studies where some of the expectations are not supported or where the results oppose theoretical hypotheses. Ifinedo (2011) found support for the importance of most the constructs of PMT, except for response cost, in explaining compliance intention. However, contrary to expectations the perceived severity of threat decreased the compliance intentions instead of increasing them. The perceived susceptibility has also had an unexpected negative impact on a variety of security practices while greater perceived severity predicted practices as expected in the theory (Crossler & Bélanger, 2014). They also noticed that greater response efficacy and self-efficacy predicted better security practices, but response cost was not a significant predictor. Liang and Xue (2010) found that both threat appraisals (perceived susceptibility and severity) and coping appraisals (response efficacy, response cost, and self-efficacy) were

significant predictors of threat avoidance behaviours. Other studies also found that confidence in security behaviours (self-efficacy), concern about security threats (threat susceptibility) predicted attitudes toward security related behaviours (Anderson & Agarwal, 2010). There have been studies where response efficacy has not been a significant predictor of adaptive response intention, while severity, susceptibility and self-efficacy have (Siponen, Mahmood & Pahnila, 2014).

Furthermore, Workman (2009) noticed that greater personal susceptibility to security threats and greater self-efficacy resulted in more positive attitudes towards security behaviour. In the study, perceived severity was not a significant predictor of adaptive behaviour intentions. In comparison, perceived severity but not perceived vulnerability was a significant predictor of ISP compliance intention in the study by Vance et al. (2012). Their study also showed the significance of benefits and response costs (negative association) and response efficacy and self-efficacy (positive association) in explaining adaptive behaviour intentions. Self-efficacy has explained significantly secure behavioural intentions almost in every study, but, interestingly, in the study by Kim et al. (2014), this relationship was not detected. High self-efficacy regarding one's own capability to take care of security-related issues can also have a negative effect on adoption intention (Herath, Chen, Wang, Banjara, Wilbur & Rao, 2014). In their study, threat appraisal and response efficacy were positively associated with the intention to adopt security behaviour.

It has also been noticed that threat and coping appraisal processes have an influence on each other. High perceived threat severity predicted lower self-efficacy and lower evaluation of response efficacy, which in turn increased behavioural intentions to act securely (Johnston & Warkentin, 2010). However, this study will only focus on the relationship between appraisal processes and chosen behaviour.

In summary of the research on PMT in the information security field, all of the constructs in PMT have been noticed to be significant predictors of security intentions and behaviours in some studies, but not necessarily in all cases. It is possible that the discrepancy between findings is due to the differences in their contexts: certain constructs could be important with regards to certain behaviours while other factors are needed with different behaviours. It is possible that the results would be clear and concise if context-specific factors would be taken into account in interpreting results. A few studies have indeed found differences in the importance of threat and coping appraisals in different contexts. Lee and Larsen (2009)

investigated the effects of threat and coping appraisals on users' decisions to adopt anti-malware software for their organization, and found that threat appraisal was more central for the adoption intention of IS experts and IT-intensive industries while coping appraisal was more important for non-IS experts and non-IT intensive industries. Threat appraisal has also been a stronger motivator for adopting anti-plagiarism software in universities than coping appraisal (Lee, 2011).

The results of Boss, Galletta, Lowry, Moody and Polak (2015), with regard to the significance of explanatory factors, differed in a few respects according to the security behaviour in question, and also in relation to the fear-appeal manipulation. When all the fear appeal manipulations were combined, only the perceived severity of threat (which increased the probability) and response costs (which decreased the probability) explained back-up intentions while anti-malware software use intentions were predicted by response efficacy (increased the probability) and response costs (decreased the probability). In both models, intentions predicted actual behaviours. However, in the high fear appeal manipulation, all of the constructs in PMT were significant explanatory factors for both back-up intentions and anti-malware software use intentions (Boss et al., 2015). In the low fear-appeal manipulations, only response costs and threat vulnerability were significant predictors of back-up intentions; while for software use intentions all the constructs were significant, except threat severity and threat vulnerability as direct predictors of intentions. The study by Boss et al. (2015) shows that the strength of fear appeal is a very important factor which affects the result of the study, and that explanatory factors could differ for different types of security behaviours, so this study is focusing on the security behaviour of LBSN users with respect to the use of privacy settings.

2.6 Hypothesis Development

Based on the body of literature around PMT, the following hypotheses are formulated. In the present study, the theoretical expectations are tested for adaptive behaviour.

Past research shows that **perceived risk severity** positively influences the security practices of individuals. In one study, when investigating the intentions for users to adopt anti-malware software, perceived severity had a positive relationship with intentions to adopt anti-malware software (Kumar et al., 2008). These results are consistent with other studies which found

that concern about security threats positively influence security attitudes, which positively affect intentions to perform security behaviours (Anderson & Agarwal, 2010). Another study found that perceived severity positively affected whether or not people properly secured their wireless networks (Woon et al., 2005). The result of a survey also showed that the perceived risk of threats, which could exploit the users' information, was a heavy influence on the decision to change, overriding any influence of benefits (Floyd et al., 2000). 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 expected that perceived severity will positively influence the use of privacy settings. Hence:

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 actually affects these practices. In one study, perceived susceptibility was shown to positively affect intentions to adopt anti-malware software (Kumar et al., 2008). Johnson et al. (2015) also suggested that the perceived susceptibility of risky behaviour will have a positive influence on the user's intention to engage in the recommended action as described in the fear appeal. When explaining whether people will comply with security policies, perceived vulnerability did not have a significant relationship with security attitudes (Herath & Rao, 2009b). 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, even with the mixed findings from prior research, it is expected that perceived susceptibility will positively influence individuals' intention to adopt a protective behaviour. Hence:

H2: Perceived risk susceptibility will positively influence the use of LBSN privacy settings.

Fear, a negative emotional response, is as a result of 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. Hence:

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 (McIntosh et al., 1997; Osman et al., 1994; Rogers, 1975; Witte et al., 1996). Hence:

H5: An increase in fear will positively influence the use of LBSN privacy settings.

Sharing Benefits. 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. The study was on the dangers of sun tanning (Leary & Jones, 1993). The result showed that people who had high concerns for their appearance and enjoyed sunbathing were less likely to take precautions for sun exposure, while at the same time noting the potential danger involved with the activity. This result supports the statement made by Marett et al. (2011) that the enjoyment gained from risky behaviours may simply be of stronger value for users than the perceived risk. In relation to this study it implies that users who enjoy sharing their location information on their profile on LBSN are less likely to make the adaptive change for protection. 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 means the belief in one's ability and willpower to make the recommended behavioural change to produce outcome (Bandura, 1977). Since its initial conceptualization, a number of studies have applied the concept of self-efficacy to explain individuals' performance at using computers (Carlson & Grabowski, 1992; Compeau et al., 1999; Compeau & Higgins, 1995; Fagan et al., 2003; Fenech, 1998; Johnson & Marakas, 2000; Lee et al., 2003; Stephens, 2005). PMT research has found similar results when relying on self-

efficacy to explain performance of security tasks. Self-efficacy has a positive relationship with users' intentions to adopt anti-malware software (Kumar et al., 2008). 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, 2009b). Similar to these findings, other research found a positive relationship between self-efficacy and security behaviour (Anderson & Agarwal, 2010). Hence:

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. IS research has found support for these findings with the intentions of users to adopt anti-malware software being lower when response cost is high (Kumar et al. 2008). Further 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). These findings are in line with other security research where a security countermeasure will not occur when the cost of responding to a security threat is greater than the damage of the resulting threat (Lee et al., 2002). This is similar to technology adoption literature, which shows that as the cost for using a technology increases, an individual becomes less likely to use the technology (Ghorab, 1997; Reardon & Davidson, 2007; Wu & Wang, 2005). Such findings from previous research suggest that as the cost of invoking a coping response increases, then the likelihood of implementing the response goes down. In other words, if an individual perceives the use of privacy settings as time consuming and effort involved with using privacy settings as being more tedious than the consequences of the threat itself, he is less likely to engage in an adaptive response. 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 some IS studies represent a "person's estimate that a given behaviour will lead to certain outcomes" (Bandura, 1977),

and it has been found to be relevant in terms of technology acceptance (Chung et al., 2002; Compeau et al., 1999; Compeau & Higgins, 1995b; Lam & Lee, 2006; Venkatesh et al., 2007). PMT research has found similar results using response efficacy to explain performance of security tasks. Response efficacy has a positive relationship with users' intentions to adopt anti-malware software (Kumar et al., 2008). Response efficacy was also 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).

Further PMT research confirms these findings with response efficacy positively influencing the use of anti-spyware software (Johnston & Warkentin, 2010) and properly securing home wireless networks (Woon et al., 2005). Consistent with these studies, other research found that response efficacy positively affected security attitude (Herath & Rao, 2009b).Hence:

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). Hence:

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.

In summary, this chapter has presented evidence for the need to motivate users to protect their location information on social networking sites using fear appeal. It also developed a set of hypotheses for understanding factors that influence users' intention to use location privacy settings. The hypotheses are summarized in Figure 5. An adaptation of PMT guided the

development of the proposed hypotheses. The following chapter explains in details the method used in this study.

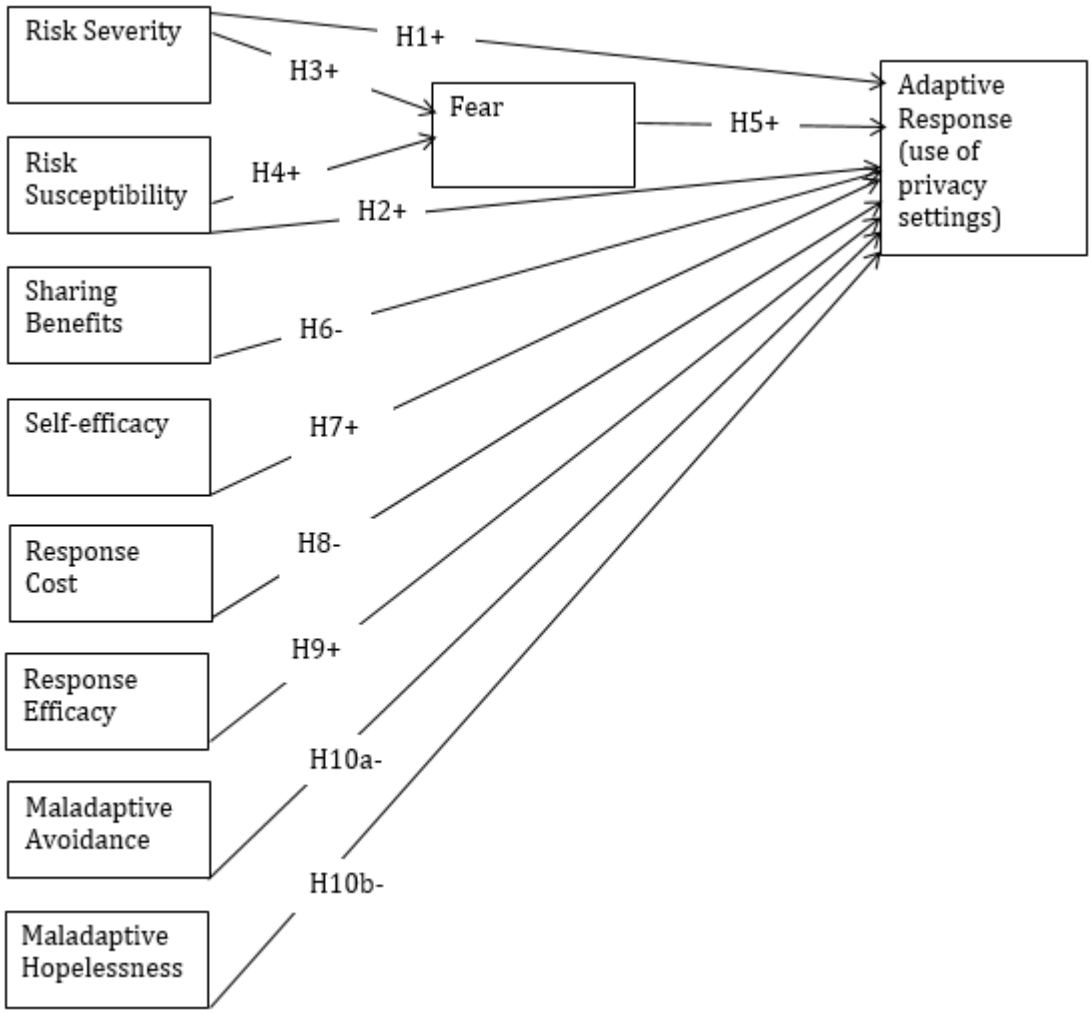


Figure 5: Research Model

3 RESEARCH METHODOLOGY

The sequence of appropriate choices selected and decisions made throughout the research process are presented and discussed (Cavana et al., 2001; Sekaran, 2003). As suggested by Myers (2009), a research design should give an overview of the road map, plans, guidelines and procedures followed in a research and these are presented in the following sections.

3.1 Research philosophy (Paradigm)

Paradigms are the mental models or frames that we use to organise our reasoning and observations. Saunders (2007) defines paradigm as the basic set of beliefs or world view that guides the investigation. According to Burrell and Morgan (1979), social-science research is shaped by two fundamental sets of philosophical assumptions: ontology and epistemology.

3.1.1 **Ontology**

Ontology refers to our assumptions about how we see the world. According to Saunders et al. (2007) there are two aspects of ontology: objectivism and subjectivism.

The ontological stance taken for this study is objectivism. Objectivism portrays the position that social entities exist in reality independent of social actors concerned with their existence and that the nature of these social actors can be measured and characterized (Saunders et al., 2009; Orlikowski & Baroudi, 1991).

3.1.2 **Epistemology**

Epistemology refers to our assumptions about the best way to study the world. Interpretivist, critical realist, positivist and pragmatist are the major epistemology stances that exist in social science research (Creswell, 2009). The researcher adopted a positivistic stance as the aim of this study is to objectively examine and measure the impact of fear appeal on the use of privacy settings in LBSNs. A positivist believes that knowledge is available and can be observed and measured objectively. It further posits that by focusing on causality, the phenomena of interest can be reduced to its simplest elements. According to Orlikowski and Baroudi (1991), a positivistic study is one in which there is a quantifiable measure of variables and one where inferences are made about a phenomenon from the

stated sample of a target population. This is in line with this study as there will be an empirical measurement of the relationship between the independent variables (perceived risk severity, perceived risk susceptibility, benefits, self-efficacy, response efficacy and response cost) and the dependent variable (behavioural intention of the use of privacy settings in LBSNs) after being exposed to fear appeal. These relationships exist in literature (Marett et al., 2011; Johnson & Warkentin, 2010) and the measurement of the patterns can be carried out objectively. Therefore, the researcher took an objective approach whereby there was no involvement with the objects of study and tests were carried out empirically.

3.2 Purpose of Research

According to Neuman (1994), if a researcher is trying to describe a phenomenon, the research is said to be descriptive, if he or she is trying to explore a new phenomenon, the research is said to be exploratory, if he or she is trying to explain why something occurs the research is said to be explanatory (Neuman, 1994).

The purpose of this research is explanatory. An explanatory research is devoted to finding causal relationships among variables. It does so from theory-based expectations on how and why variables should be related. Hypotheses could be basic (i.e. relationships exist) or could be directional (i.e. positive or negative) (Malhotra, 1998). This explanatory study explains, hypothesizes, and test for a positive and negative relationship between the independent and dependent variables. Results then are interpreted and in turn contribute to theory development.

3.3 Research Approach

Deductive and inductive approaches are the two major approaches used in building and testing theories in research. A deductive approach was applied in this study. This approach is suitable because this study is not based on developing new theory as is the case for inductive approach (Creswell, 2009) but rather seeking to test the conceptual model informed by literature and existing theoretical work (Creswell, 2009). This approach involves developing hypothesis based on existing theoretical work and testing these propositions to either confirm or reject them (Bhattacherjee, 2012). This research followed this approach by conducting an extensive review of literature on key areas in relation to the topic of study. Some variables were adapted from PMT while the others were informed by literature. This

resulted in the development of a conceptual model. The conceptual model as well as literature led to the development of twelve hypotheses that were tested using quantitative measures. From the test conducted, the findings confirmed or rejected the hypotheses as shown later in this dissertation. This research approach also served as a guide in realising the research objective and answering the research question of this study.

3.4 Research Strategy

The research strategy for this study was to carry out a survey to test the developed hypotheses, answer the research question and realize the research objective. The survey used a standardized questionnaire to collect data involving people in order to capture their perceptions and behaviours in a systematic way after the fear appeal had been issued (Bhattacherjee, 2012). This research strategy through the use of questionnaires was deemed suitable for this study because it has strength in aiding the ability to collect data about a population that is too large to observe directly. Furthermore, it supports the philosophical stance taken for this research as the researcher can carry out the research objectively, i.e. without involvement with the participants. In addition, it is economical in terms of the amount of time, efforts and cost necessary for conducting research. However, survey research has its weakness in biases that can affect the inferences derived from data. Two biases that have been recognized as potential biases for this study are non-response bias and sampling bias. These biases and how they will be addressed will be discussed later in the research design.

3.5 Sampling

Sampling is the statistical process of selecting a subset (called a 'sample') of a population of interest for purposes of making observations and statistical inferences about that population (Bhattacherjee, 2012). The entire populations cannot be studied because of feasibility and cost constraints; therefore, a representative sample must be selected from the population of interest for observation and analysis. A sample that is truly representative of the population was chosen so that the inferences derived from the sample could be generalized back to the population of interest (Bhattacherjee, 2012).

3.5.1 **Target population**

A population can be defined as all people or items (unit of analysis) with the characteristics that one wishes to study (Bhattacherjee, 2012). However, the target population is more

concerned with the specific sample to be studied. For this study the target population (unit of analysis) was LBSN users. The research targeted university of Cape Town students who were users of one or more of the common LBSNs. This was because previous research showed that the majority of frequent LBSN users were between the ages of 15 and 35 (Harris Interactive, 2010). Due to the ethical issues involved with studying minors, the research decided to only include a sample of individuals who were 18 years and above. In addition, the researcher also believed that the technical know – how and level of exposure in terms of the nature of constructs being observed for this study would be better understood and relatable with educated LBSN users.

3.5.2 **Sampling frame and sample size**

A complete and accessible list of information about the cases of the target population of a study from which the sample will be drawn from is referred to as a sampling frame. The researcher contacted the research office in order to get access to students of the University of Cape Town from which the study sample was drawn. Saunders et al. (2007) suggest that in order to have a representative sample that has a low and tolerable margin of error, one should aim for large sample sizes. However, studies relating to online social networking in general had an average sample size of 200+ users. The sample size for this dissertation was 248 social networking site-users in the University of Cape Town. The research shows through analysis that this number is sufficient to ensure a representative sample size and a low margin of error.

3.6 Data collection and instruments

This dissertation used quantitative methods as a means of data collection and testing the conceptual model by examining the relationship among variables. Certain types of social research problems call for specific approach; if a research calls for identification of factors that influence an outcome or understanding the impact of a specific variable on an outcome then a quantitative approach is best suitable (Creswell, 2009). It is also the best approach used to test a theory. The variables in the conceptual model was measured typically on the instruments adapted so that numeric data could be analysed using statistical procedures. The research philosophy adopted for this dissertation also guided the choice of quantitative method as the primary means of data collection and research instrument. Questionnaires was used as the instrument for collecting data for this dissertation. The questionnaire was

prepared based on instruments used in previous studies examining fear appeal using PMT and modified for the context of location-based social networks (Marett, 2011; Boss et al., Johnson & Warkentin, 2010; Johnson, 2015). The resulting instruments was reviewed and reworded by the researcher to ensure more clarity and capture the purpose for the dissertation.

A pilot survey consisting of a convenience sample of 10 participants (five males and five females, in three age groups) was conducted in order to confirm that the wording of questions was appropriate. Some questions were highlighted as problematic, and a second pilot was run after some questions were either rephrased or removed.

A Fear appeal was issued to the participants prior to answering the questions. The fear appeal was adapted from studies by Marett (2011), and Johnson (2010). The fear appeal used can be found in Appendix C**.** To ensure that the participants read and understood the fear appeal, the survey required subjects to correctly answer open-ended questions about its content before they could proceed. Questionnaires was issued to the participants to measure the impact of fear appeal on the use of privacy settings in LBSNs. The questionnaire contained demographic questions and variables from the conceptual model which includes perceived risk severity, perceived risk susceptibility, response costs, benefits, response efficacy, and self-efficacy.

The item of each construct in the framework was measured using closed-ended questions. A five-point Likert scale was used to measure the items with 1 and 5 representing the lowest (Strongly Disagree) and highest (Strongly Agree) values respectively. Table 1 illustrates the match of items of the construct and hypotheses in the questionnaire. The research instrument is presented in Appendix D.

The researcher made use of Qualtrics to distribute the questionnaires. Qualtrics is a web-based survey service which allows easy creation of survey, online collection and storage of data (Qualtrics, 2016). This eliminated cost, saved time and ensured a wide reach of the subjects. Table 1 shows the questions and studies they were adapted from:

Table 1: Variables, Questions and Sources

	Variables (Source)	Questions
1	Risk Severity (Marett, 2011)	In general, it is risky to disclose my location information on a LBSN.
		There would be high potential for loss associated with posting my location information on LBSNs.
		It is uncertain who might have access to my location information on LBSNs.
		Posting my location information on LBSNs would involve many unexpected problems.
2	Risk Susceptibility (Johnston and Warkentin 2010)	My privacy is at risk when disclosing location information.
		It is possible that I become a victim.
		It is likely that I become a victim.
3	Benefits (Marett 2011)	I enjoy sharing my location information with others.
		Sharing my location information with others is fun to do.
		Sharing my location information with others is a boring activity (reverse coded).
		Sharing my location information with others does not hold my attention at all (reverse coded).
		I would describe sharing my location information with others as interesting.
		I think sharing my location information with others is quite enjoyable.
		I earn respect from others by sharing my location information with them.
		I feel sharing my location information with others improves my status within my group of friends.
		I share my location information with others to improve my reputation.
4	Self-efficacy (Johnston & Warkentin, 2010)	I have the ability to use privacy settings without much effort.
		Privacy settings are easy to use.
		Privacy settings are convenient to use.
5		Using privacy settings works for protection.

	Response Efficacy (Johnston & Warkentin, 2010)	Privacy settings are effective for protection.
		When using privacy settings, my location information is more likely to be protected.
6	Response Cost (Woon et al., 2005)	Using privacy settings would require a considerable amount of effort other than time.
		There is too much work associated with trying to increase my information protection through the use of privacy settings.
		Using privacy settings would be time consuming.
7	Fear (Marett et al., 2011; Osman et al., 1994; Milne et al., 2002)	I feel frightened by the potential dangers associated with disclosing my location information on LBSNs.
		Knowing that people have been victims in the past is terrifying.
		I am worried about the prospect of being a victim.
8	Adaptive Response: intention to use privacy settings (Johnson & Warkentin, 2010)	In future I intend using privacy settings to control access to my location information.
		In future I predict using privacy settings.
		In future I plan on using privacy settings.
9	Maladaptive Response: avoidance (Marett et al., 2011**;** Myyry et al., 2009)	I try not to think about the potential danger of not using my privacy settings.
		I am not at risk from the potential danger of posting my location information on LBSN.
		Not using privacy settings saves me time.
10	Maladaptive response: hopelessness (Marett et al., 2011)	There is nothing I can do to avoid the potential dangers associated with disclosing my location information on LBSN.
		I feel it is useless to use privacy settings to protect myself from the potential dangers associated with LBSNs.
		I am at a loss as to how to use privacy settings to protect myself from the potential dangers associated with LBSNs.

3.7 Reliability and Validity of Research Instrument

According to Moore and Benbasat (1991), there are two stages required to ensure the reliability and validity of the constructs of the measurement instruments. The first stage requires the identification of existing items or the creation of new ones and the second step demands the assessment of construct validity.

The purpose of reliability is to determine the consistency and dependability of measures of the construct (Neuman, 1994; Bhattacherjee, 2012). According to Creswell (2008), if an instrument of research has been modified, the reliability and validity used in the study which it was adapted from may not hold for the new instrument therefore during the data analysis of the current study, a validity and reliability test is required. According to Bhattacherjee (2012), there are four ways to test reliability: split-half reliability, inter-rater reliability, internal-consistency reliability and test-retest reliability. Internal-consistency reliability was used to test the reliability of the instrument used in this research. This test was done by measuring the various items of a construct to check for consistency. The measurement was done by calculating the Cronbach's Alpha and Composite Reliability (CR). The researcher chose these tests because both are endorsed by academics and the results are reliable. The researcher also increased the reliability by conceptualizing the construct clearly and carrying out a pilot test (Neuman, 1994). The researcher ensured that the constructs being measured were clearly defined in the literature review. According to Neuman (1994), each measure should only indicate one concept and a clear theoretical definition of the construct should be given. Composite reliability scores equal to or greater than 0.70 are regarded as acceptable (Gefen & Straub, 2005).

Validity involves the level of adequacy of a measure in representing the construct meant to be measured. There are validity test conducted for hypotheses testing procedure and validity test conducted for measurement procedures (Bhattacherjee, 2012). Construct validity and content validity was used as the measurement procedure in this study. Content validity checks that the full definition of a construct is represented in a measure. Construct validity addresses whether generalisations can be made from the measurement questions to the constructs. In other words, do the measurement questions truly measure the presence of the constructs they are meant to measure? This follows the suggestion by Bhattacherjee (2012) as these validity tests do not have a direct measurement but can be

ensured by consulting experts in the research field. Factor loadings were examined to ensure that items loaded correctly on the constructs to which they were intended to load, and did not cross-load on constructs to which they were not to load (Straub et al. 2004).

In addition to the above tests, the researcher was aware of the threats to validity that could have arose, therefore, internal validity, external validity and statistical validity was checked and accounted for (Creswell, 2009). In regards to internal validity, which checks the appropriateness and ability to draw inferences from the target population (Bhattacherjee, 2012), the sampling technique for this research helped to ensure that the characteristics of the participants was equally distributed. Furthermore, the researcher aimed to get a large amount of respondents that would be suitable for this purpose. External validity checked that no incorrect inferences were made from the sample data (Bhattacherjee, 2012). In light of these, the researcher had ensured that there was an adequate level of representativeness in the sample based on the sample frame and the demographics section of the research instrument. With a careful selection of adequate statistical measurements, the statistical validity was ensured.

Response data was used for these validity tests. For tests of convergent validity of the variables, patterns of correlation between items and constructs were examined (Petter et al., 2007).

Discriminant validity ensures that a construct measure is empirically unique and represents phenomena of interest that other measures in a structural equation model do not capture (Hair et al., 2010). If discriminant validity is not established, “constructs may have an influence on the variation of more than just the observed variables to which they are theoretically related” and, as a consequence, “researchers cannot be certain results confirming hypothesized structural paths are real or whether they are a result of statistical discrepancies” (Farrell, 2010, p. 324).

Discriminant validity was assessed by analysing item cross-loadings at the indicator level. Each item in this study loaded highest on its respective loading to ensure discriminant validity (Gefen et al., 2000; Straub et al., 2004). Discriminant validity was assessed at the construct level by comparing the square root of each construct's average variance extracted against its correlation with other constructs (Fornell & Larcker, 1981).

3.7.1 Manipulation Check

To ensure that the subjects of the survey were successfully manipulated by the fear appeal treatment, a general question as to whether or not they completely read and understood the fear appeal was asked. A discriminant analysis of the variables threat severity, threat susceptibility, self-efficacy, and response efficacy, using subject responses to the general question as a grouping variable was conducted. The following sections detail the data analysis procedures involved in this study.

3.8 Data Analysis Technique

Analysis of the data gathered from the questionnaire was done through the use of quantitative measures and technique because the research instrument consists of quantifiable data. The survey's data was exported from Qualtrics into Microsoft Excel. To ensure the data set was free of error, a data-cleaning process was done in which rows which had blank, incomplete data or uniform answers all through were removed. After satisfactory data cleaning, the names of the indicators were placed in the first row of the spreadsheet to ensure that SmartPLS (a statistical software) was able to import the data properly. Since SmartPLS cannot import the native Excel file format directly, the data set was converted into '.csv' file format.

The prepared data was then captured and analysed using 'SmartPLS3' a Partial Least Square Structural Equation Modelling (PLS-SEM) software package (Ringle et al., 2005). The researcher chose SmartPLS because it is widely used for statistical analysis, it is easily accessible and the researcher has understanding of the software.

The Partial Least Squares technique of structural equation modeling, utilizes a principle component-based for estimation. PLS-SEM is "an ordinary least squares (OLS) regression-based method which uses available data to estimate the path relationships in the model" (Hair, Ringle, & Sarstedt, 2013, p. 14). The approach is suitable for validating predictive models, especially those with small sample size (Chin, 1998). PLS supports two models: (a) the assessment of the measurement model and (b) the assessment of the structural model. The advantage of this approach lies in the fact that with SEM, the measurement and the structural model can be analyzed at once (Hair et al., 2013). Furthermore, the decision for SEM, based on the underlying approach of PLS, was due to the research aims, which was to

explain the variance of the endogenous construct 'use privacy settings after being issued with a fear appeal' (Chin, 1998). Furthermore, PLS has fewer stringent requirements regarding distribution properties (Wold, Martens & Wold, 1983). SmartPLS generates t-statistics for significant testing of both the inner and outer model using a procedure called bootstrapping (Wong, 2013).

3.9 Timeframe

The timeline for a research project can either be cross-sectional or longitudinal. A cross-sectional time dimension involves collecting data at a particular period of time which does not exceed months; while a longitudinal time dimension involves collecting data over a long time period (usually years) to study a phenomenon (Sekaran, 2003). This research was done by using a cross-sectional time dimension as the study was concerned with gaining understanding from present occurrences and present time (Saunders et al., 2009). This was deemed appropriate because of the time constraint in the Master's programme and also in line with the survey method applied for this study (Saunders et al., 2007).

3.10 Ethics and Confidentiality

In the context of research, ethics refers to the appropriateness of the researcher's behaviour in relation to the rights of those who become the subject of his work, or are affected by it (Saunders, 2007). Researchers are expected to be aware of and abide by general agreements of the research community on what constitutes acceptable and non-acceptable behaviours in the professional conduct of research (Bhattacherjee, 2012). A researcher must not manipulate his data collection, analysis, and interpretation procedures in a way that contradicts research principles or advances their personal agenda. Flagrant disregard of research etiquette can result in editorial sanctions, professional embarrassment and/or legal action (Bhattacherjee, 2012).

In conducting any research, integrity and concern for the subject are important (Neuman, 1994; Bhattacherjee, 2012). Therefore, before the instrument was distributed, it was sent to the ethics committee of University of Cape Town for review along with an ethics application form and a request to conduct the research. The approval can be found in Appendix A.

Other ethical procedures for conducting research were strictly followed and potential ethical concerns were looked out for. A cover letter containing a summary of the research introduction and purpose, the researcher's profile co-signed by the researcher's supervisor and a consent form for the participant was attached to every questionnaire served (See Appendix B). The researcher informed the participants of their voluntary choice to participate in the survey. The researcher also let the participants know that their responses will be treated with anonymity. Although the identity of the participants in this study was anonymous, demographic information was disclosed and used in assessing and analysing the data collected. The raw data collected was treated with strict confidentiality and was in the sole possession of the researcher and will be disposed after the study has been completed.

3.11 **Summary**

The objective of this research was to identify the impact of fear appeal on the factors that influence the use of privacy settings in LBSNs. In light of this, this chapter has provided an overview of the research design and methodology adopted for this research; it has also shed light on the philosophical underpinnings for research which determine the choice of research paradigms, methods, approaches and techniques adopted for a study. This research adopted a positivistic paradigm, a survey strategy, an explanatory research and the use of quantitative methods for data collection and analysis. The research instrument involved closed-ended questions.

4 DATA ANALYSIS

This chapter presents the data analysis procedures involved in this study and a discussion of the results. Included in this discussion are descriptions of instrument validity tests and reliability test. Following the description of the analyses, the results are presented in model and tabular format. This chapter ends with a discussion of the findings, which includes the similarities and differences between the findings of this study and previous studies.

4.1 Demographic Analysis

A total of 452 questionnaire responses was collected. Some of the responses were incomplete and were deleted, leaving a final selection of 248 responses which were used for data analysis. Respondents who partook in the survey were all university students. They were asked to indicate their gender, age, and their experience using social networking sites. The information derived from the responses to these demographic categories is presented in Table 2.

Table 2: Respondent Demography

Demography	Category	Frequency	Percentage (percent)
Gender	Male	99	39.9
	Female	149	60.1
Experience	1 to 12 months	27	10.9
	> 1 year to 2 years	22	8.9
	> 2 years to 3 years	27	10.9
	> 3 years	172	69.4
Age	<18	4	1.6
	18 to 20	97	39.1
	21 to 25	77	31.1
	26 to 30	28	11.3
	30<	42	16.9

Of the 248 respondents, the majority (149) was female as shown in Table 1, followed by a count of 99 who were males. As shown in the Table above, most respondents (172) had been using social-networking sites for more than three years. The age group of 18 to 20 had

the highest count, with a frequency of 97 respondents. This is a representative of social networking sites users according to survey of other studies (Tufekci, 2008; Saeri et al., 2014, Mohamed et al., 2012; Marett, 2011)

4.2 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 (Haenlein & Kaplan, 2004; Hair et al., 2013; Petter et al., 2007).

4.2.1 **Internal consistency reliability**

Internal-consistency reliability is a measure of consistency between different items of the same construct (Bhattacherjee, 2012). When a multiple-item construct measure is administered to respondents, the extent to which respondents rate those items in a similar manner is a reflection of internal consistency. The internal consistency of the variables used to measure each construct was first determined using Cronbach's Alpha test. This has been employed to determine the reliability of variables to check that they are dependable and consistent (Bhattacherjee, 2012). A threshold of 0.70 is normally used and is the acceptable value of Cronbach's Alpha; however, a threshold of 0.60 can be considered in the case of an exploratory research (Fornell & Larcker, 1981; Hair et al., 2006). Column 3 in Table 2 shows the results of Cronbach's Alpha test on each construct.

Table 3 Construct Reliability

Variables	No of items/indicators measured	Cronbach's Alpha	Composite Reliability
Adaptive Response	3	0.9	0.96
Sharing Benefits	8	0.8	0.93
Fear	3	0.8	0.87
Maladaptive Avoidance	3	0.5	0.74
Maladaptive Hopelessness	3	0.8	0.86
Response Cost	3	0.9	0.91
Response Efficacy	3	0.8	0.85

Self-efficacy	3	0.9	0.91
Risk Severity	3	0.7	0.83
Risk Susceptibility	3	0.7	0.83

These scores suggest that all but maladaptive avoidance have a reliability of 0.7 and above. Although 0.5 Cronbach alpha reliability result for maladaptive avoidance is low, it has generally been stated that Cronbach's alpha gives a lower bound to the true reliability (Sijtsma, 2009). Traditionally, Cronbach's Alpha is used to measure internal consistency reliability in social science research but it tends to provide conservative measurement in PLS-SEM. Studies have suggested the use of Composite Reliability as a replacement (Bagozzi & Yi, 1988; KKK Wong, 2013; Hair et al., 2012).

Composite reliability was used to determine the reliability of variables by evaluating the internal consistency of the reflective measurement model (Henseler et al., 2009; Hair et al., 2011). Composite reliability scores equal to or greater than 0.70 are regarded as acceptable (Fornell & Larker, 1981; Gefen & Straub, 2005). Reliability for the scales was also gauged via composite reliability scores provided in the PLS output. As indicated in column 4 Table 2, the composite reliability scores of the variables are greater than 0.7. Therefore, high levels of internal consistency reliability have been demonstrated among all the variables.

Indicator reliability was assessed by examining the outer loadings. Each indicator's loading should be higher than 0.70 (Hair et al., 2011). All but six indicators were above the 0.70 threshold and the impact of deleting the six indicators was examined. Two indicators (Question 4 measuring *benefits* and Question 4 measuring *risk severity*) were removed (outer loading < 0.30) but the others were kept as no significant increase in CR or AVE was achieved (Hair et al., 2014).

4.2.2 **Convergent Validity**

Convergent validity refers to the closeness with which a measure relates to (or converges on) the construct that it is purported to measure (Bhattacherjee, 2012). Convergent validity is demonstrated if (1) the item loadings are in excess of 0.70 on their respective factors and (2) average variance extracted (AVE) for each construct is above 0.50 (Gefen & Straub, 2005). Each latent variable's AVE was evaluated to check the convergent validity. The AVE criteria as shown in Table 4 Column 2 are all above the recommended threshold (0.5), which

indicates that, on average, the construct explains more than half of the variance of its indicators hence convergent validity was confirmed.

4.2.3 **Discriminant Validity**

Discriminant validity refers to the degree to which a measure does not measure other constructs that it is not supposed to measure (Bhattacherjee, 2012). Discriminant validity can be established if (1) item-to-variable correlations are higher with each other than with other variable measures and their composite values and (2) the square root of each variable's AVE is greater than other correlations among the latent variable (Gefen & Straub, 2005). AVE represents the average amount of variance that a construct explains in its indicator variables relative to the overall variance of its indicators.

To assess discriminant validity, the Fornell-Larcker criterion was first used. This is a more conservative approach to cross loadings and was considered appropriate since all variables are reflective (Hair et al., 2014). Fornell and Larcker (1981) suggested that discriminant validity is established if a latent variable accounts for more variance in its associated indicator variables than it shares with other constructs in the same model. To satisfy this requirement, each construct's AVE must be compared with its squared correlations with other constructs in the model (Gefen & Straub, 2005). The results are indicated in Column 3-12 of Table 4.

Next the researcher followed the recommendation of Henseler, Ringle and Sarstedt (2015). It examined the heterotrait-monotrait (HTMT) ratio of correlations which is the average of the heterotrait-heteromethod correlations (i.e. the correlations of indicators across constructs measuring different phenomena), relative to the average of the monotrait-heteromethod correlations (i.e. the correlations of indicators within the same construct) to assess discriminant validity. HTMT discriminant validity involves comparing it to a predefined threshold. If the value of the HTMT is higher than this threshold, one can conclude that there is a lack of discriminant validity. Research scholars suggest a threshold of 0.85 (Clark & Watson, 1995; Kline, 2011). All values were below the conservative 0.85 threshold level (Kline, 2011), thus confirming that discriminant validity had been established.

Table 4 presents a summary of the assessment results, showing AVE in Column 2, and Fornell-Larcker results in Columns 3-12.

Table 4: Assessment of Reflective Measurement Model

	AVE	AR	BF	F	MA	MH	RC	RE	SE	SV	SUS
Adaptive response (AR)	0.90	0.95									
Benefits (BF)	0.61	-0.33	0.78								
Fear (F)	0.69	0.28	-0.25	0.83							
Maladaptive Response Avoidance (MA)	0.50	-0.39	0.30	-0.17	0.70						
Maladaptive Response Hopelessness (MH)	0.67	-0.39	0.28	-0.12	0.52	0.82					
Response Cost (RC)	0.76	-0.20	0.18	-0.02	0.46	0.50	0.87				
Response Efficacy (RE)	0.65	0.30	-0.003	0.08	-0.03	-0.20	-0.15	0.80			
Self-efficacy (SE)	0.77	0.26	-0.08	-0.02	-0.30	-0.25	-0.58	0.30	0.88		
Risk Severity (SV)	0.63	0.36	-0.36	0.57	-0.24	-0.15	-0.02	0.15	0.04	0.79	
Risk Susceptibility (SUS)	0.61	0.35	-0.33	0.58	-0.24	-0.08	0.02	0.04	-0.004	0.60	0.78

For example, the latent variable *response cost's* AVE is found to be 0.76, with its square root being 0.87 (Fornell-Larcker criterion). This number is larger than the correlation values in the column of *response* cost and also larger than those in the row of *response cost.* Similar observation is also made for the other latent variables. This result indicates that discriminant validity is well established.

4.3 Analysis of the Structural Model

The structural model was tested using SmartPLS to estimate the path coefficients, which calculates the strength of the relationships between independent and dependent variables. The weight of different path coefficients enables us to rank their relative statistical importance. R-squared values were also estimated, in order to display the variance explained by the independent variables. The PLS path modelling estimation for the research is shown in Figure 1. By examining the results, the following observations were made:

4.3.1 Explanation of target endogenous variable variance

The value 0.372 presents the coefficient of determination R^2 for the *use of privacy settings* endogenous latent variable. This means that the latent variables (Sharing *Benefits, fear, maladaptive avoidance, maladaptive hopelessness, response cost, response efficacy, self-efficacy, severity and susceptibility)* explains approximately 37 percent of the variance in *use*

of privacy settings. This value is moderate according to recommendations in research (Hair et al., 2013).

Risk severity and Risk susceptibility together explains approximately 42 percent of the variance of *Fear.* This can be described as moderate according to general recommendations in scholarly research (Hair et al., 2013). However, compared to previous studies with similar constructs, in the discipline, the values show a medium to high effect size (Boss et al., 2015; Marcoulides & Saunders, 2006).

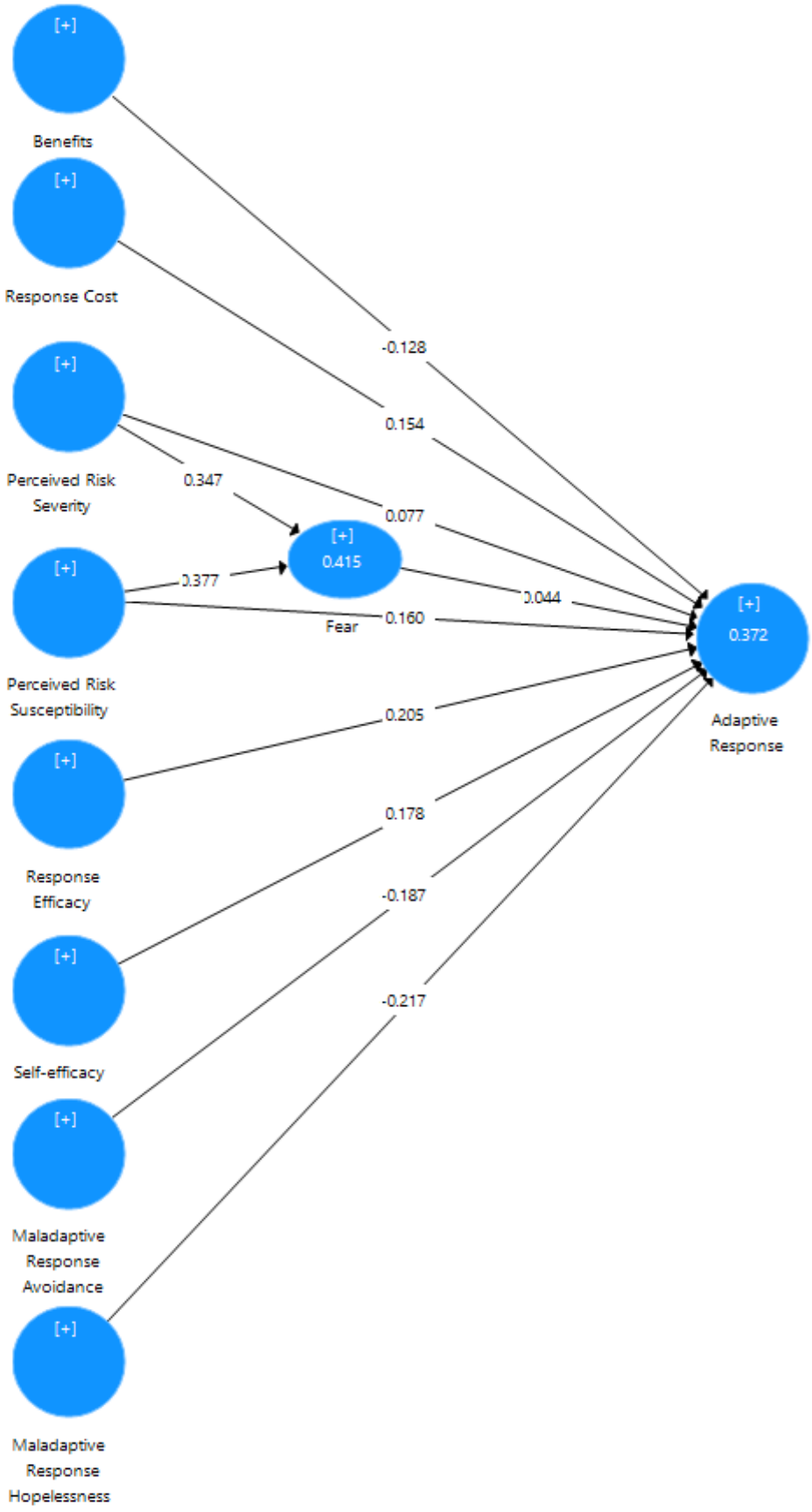


Figure 6: PLS-SEM Results showing path coefficients and coefficient of determination.

4.3.2 **Bootstrapping**

Bootstrapping was used to generate T-statistics to test the significance of both the structural path and its associated hypotheses. As recommended by (Henseler et al., 2009), 5000 subsamples were taken from the original sample with replacement to give bootstrap standard errors, which in turn gives approximate T-values for significance testing of the structural path. The bootstrapping results approximate the normality of data (Ken Kwong-Kay Wong, 2013). The analyses produce estimates of the explained variance in the constructs which is sufficient for assessing significance (Hair et al., 2014).

After running the bootstrapping, the T-statistics were observed to see if the path coefficients of the inner model were significant or not. Using a two-tailed t-test with a significant level of 5percent, (Levin et al., 1985) the path coefficient will be significant if the t-statistics is larger than 1.96. The bootstrapping result in Table 4 Column 3 shows that only H1 (1.104), and *H5* (0.61) are not significant. The inner model suggests that *maladaptive hopelessness* has the strongest effect on *adaptive response.* All but the hypothesized path relationships between *risk severity* and *use of privacy settings, fear and use of privacy settings* are statistically significant.

The results of the hypothesis testing are summarized in Table 4. Of the eleven hypotheses, nine were significant but only eight of the hypotheses were supported. This is because response cost's significance was in the opposite direction of hypothesized relationship. The results of the structural model analysis also confirm the negative relationships between benefits, maladaptive avoidance response and maladaptive hopelessness response on the use of privacy settings. The moderating effect of *Fear* was tested. The result of bootstrapping showed *fear* had a value of 0.572 which is lower than the threshold 1.96. Hence *fear* had no significant moderating effect between *risk severity, susceptibility* and *use of privacy settings*. Explained variance for the model was also reasonable. Overall, the study concludes that the model has received good support. Finally, a multi-group gender analysis was performed to determine its influence on the results of the study. The results of the analysis showed that there was no significant difference in terms of gender.

Hypothesis	Path Coefficient	T Statistics	P Values	Supported?
H1: Risk severity -> Use of privacy settings	0.077	1.104	p > .10	Not Supported
H2: Risk susceptibility -> Use of privacy settings	0.16	2.065	p < .05	Supported
H3: Risk severity -> Fear	0.347	4.699	p < .01	Supported
H4: Risk susceptibility -> Fear	0.377	5.585	p < .01	Supported
H5: Fear -> Use of privacy settings	0.044	0.61	p > .10	Not Supported
H6: Sharing Benefits -> Use of privacy settings	-0.128	2.39	p < .05	Supported
H7: Self-efficacy -> Use of privacy settings	0.178	2.48	p < .05	Supported
H8: Response cost -> Use of privacy settings	0.154	2.006	p < .05	Supported
H9: Response efficacy -> Use of privacy settings	0.205	4.228	p < .01	Supported
H10a: Maladaptive avoidance response -> Use of privacy settings	-0.187	2.788	p < .01	Supported
H10b: Maladaptive hopelessness response -> Use of privacy settings	-0.217	3.292	p < .001	Supported

Table 5 Overview of Findings

The results are summarized in Figure 7 below:

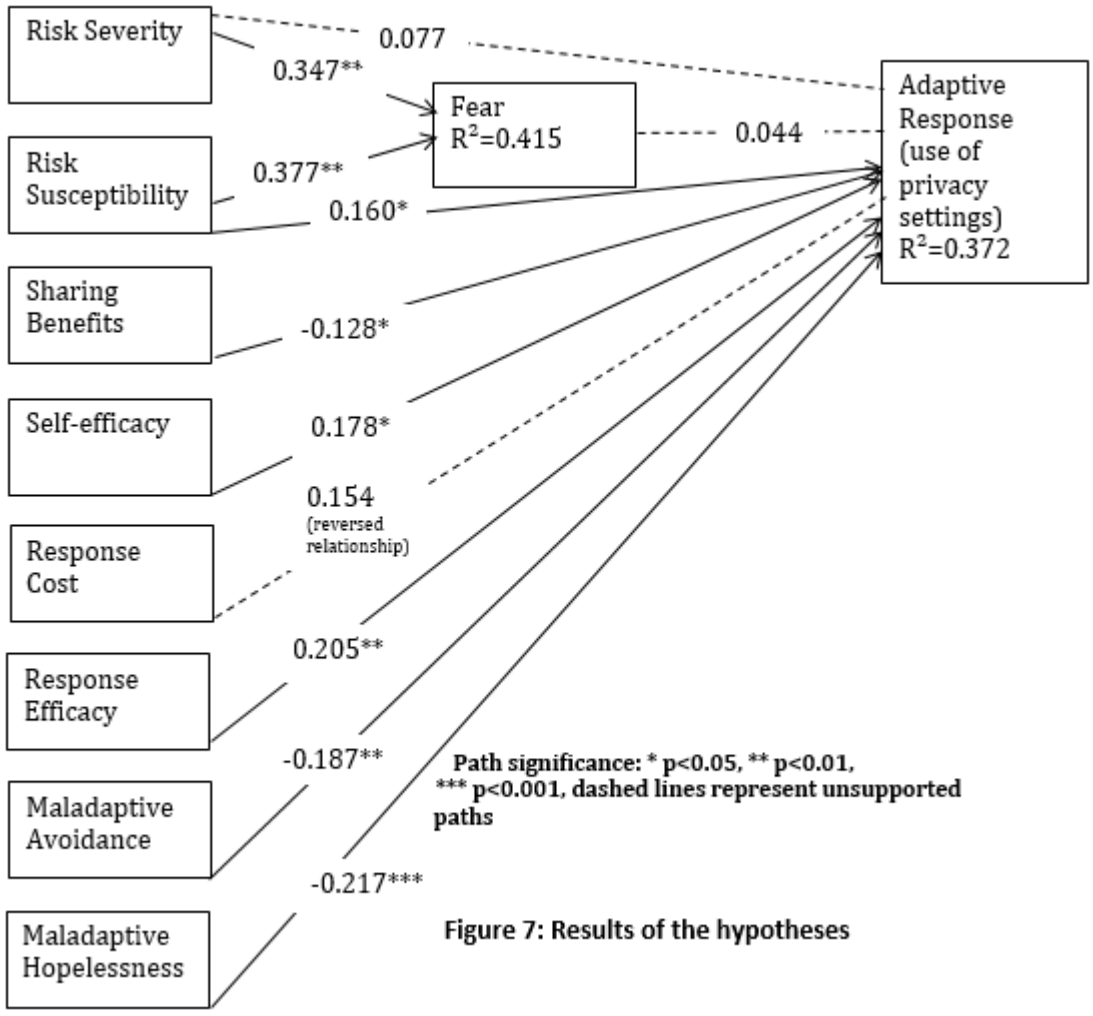


Figure 7: Results of the hypotheses

4.4 Discussion

This study empirically investigated how well PMT explained the impact of fear appeal on the use of privacy settings in location-based social networks. The constructs of PMT were hypothesized to have an effect on the use of privacy settings. It was found that PMT provides a coherent explanation of the cognitive processes used by individuals involved in social networking when presented with fear appeal. As illustrated in the analysis, the determinants proposed to have an effect on the use of privacy settings differed greatly.

4.4.1 **Threat Appraisal**

Croog and Richards (1977) suggest that users with negative experiences from the past with similar threats or knowledge of others with previous detrimental experiences can influence the perception one has of malicious outcomes. Without such cues, it is likely that a sense of invincibility may persist. As such, fear appeals should reinforce the severity of occurrences with concrete examples of the negative outcomes directly related to a threat.

The influence of perceived risk severity on the use of privacy settings was not significant. This is not a surprising result as some studies concerning the perceptions of risk severity by users found that the perceived risk severity was insignificant on the decision to change risky behaviour (Ifinedo, 2012; Liang & Xue, 2010; Lee et al., 2008; Lee & Larsen, 2009). The indication that it is not a significant determinant of adaptive behaviour is also supported in some existing studies in the health behaviour (Block & Keller, 1995; Milne et al., 2000).

It might also be possible perceived risk severity has no direct relationship with the use of privacy settings. For instance, the study by Herath and Rao (2009) and Bulgurcu et al. (2010) that examined behavioural compliance by individuals with PMT and other theories modeled concern levels and attitude as moderators of the relationship between perceived severity and behavioural compliance. Another study by (Ng et al., 2009) also found perceived severity to be insignificant on its own but significant when moderating other factors to influence computer security behaviour. These results have shown perceived risk severity to be a weak direct predictor of protective behaviour. It is possible that such a conceptualization may present a different insight to the result obtained here.

These results differ from the findings of previous studies that explored information security behaviours of working professionals which found risk severity significant (Workman, Bommer & Straub, 2008; Chenoweth, Minch & Gattiker, 2009; Ng, Kankanhalli & Xu, 2009; Herath & Rao, 2009; Johnston & Warkentin, 2010; Rifon et al., 2005; Norshidah & Hawa, 2012). The difference in results may imply that there is a distinct difference between students and working professionals in perceiving the severity of potential risks. According to a study by Marett (2011), students did not think deeply about the threat severity of their exposed information because they had little experience and perhaps a more liberal mind.

However contrary to expectations, the findings still suggest implications in identifying important factors predicting the use of privacy settings. One possible explanation is that perceived severity may not be as critical as other predictors, such as perceived susceptibility, response efficacy, self-efficacy and response cost in using protection measures. If people think posting location information leads to a serious problem, but they believe that they are not likely to be victims of online threat, then they may not use privacy settings. Given that people often tend to underestimate their chances of being victims of negative experiences, this tendency may be regarded as one of the obstacles hindering people from adopting an appropriate precautionary behaviour (Marett et al., 2011). From this perspective, the non-significant relationship between the use of privacy settings and perceived severity of online threat may suggest that users would not necessarily engage in use of privacy settings unless they believe the threats are likely to occur to them frequently and are directly related to their personal concerns about online safety, even if they believe that the threat of exposing their location information is a serious and severe issue.
However, it is also important to note that the insignificant effect of severity of online threat on use of privacy settings 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), or they just perceive that the impact losing their location information would not have a detrimental impact on them.
This indicates that focusing on the risk may lead users to ignore the protective measure, but focusing on the perceived likelihood of threat may lead consumers to opt for an adaptive behaviour. Perhaps the reason for this is that focusing on the perceived threat may increase feelings of being overwhelmed, and thus increasing the chance that a user will give up.

(Shillair et al., 2015). In this sense, negative outcome expectations may not directly influence people's willingness to use privacy settings.

Perceived risk severity had a significant influence on fear as hypothesized. As suggested in the PMT there is support for the idea that perceived risk severity enhances fear. The research result also confirms the suggestions and findings of Arthur and Quester (2004), Boss et al. (2015) and Roskos-Ewoldsen et al. (2004) as to the positive impact of perceived risk severity on fear.

Consistent with the PMT explanation (Tanner et al., 1991), the study found evidence that ***risk susceptibility*** was influential for individuals intending to change their risky behaviour. Contrary to the findings of numerous other studies, the perceived risk susceptibility which could exploit posted location information has a heavy influence on the decision to change. (Floyd et al., 2000).

Previous studies concerning the perceptions of threat susceptibility by individual users found that, in general, individuals perceive themselves to be less likely to experience a malicious attack (Loch et al., 1992; Schmidt & Arnett, 2005). Loch et al. (1992) offer that individuals often see threats as affecting others more than themselves, thus "exhibiting a rather naïve belief that bad things only happen to other people" (p. 185). The result was also contrary to some existing studies in the health behaviour (Maddux & Rogers, 1983; Milne et al., 2000). A possible explanation could be that the susceptibility of health threats differs according to the genetic makeup of the person or other personal characteristics such as age or occupation (e.g. alcohol abuse may be more detrimental to an older person or someone who already has a liver problem). However, in computer security, the impact is more uniform.

If people believed that they were vulnerable to the dangers explained in the fear appeal and that they could perform the coping response, then they intended to do so regardless of whether or not they thought the response would be effective (Maddux & Rogers, 1983). Because of their high expectations of being exposed to the danger, they were more easily persuaded by any information that offered the possibility of avoidance. Confronted with a possibility of a dangerous situation, the users seemed to be thinking they have nothing to lose by trying and thus adopted the use of privacy settings to avoid danger.

Perceived risk susceptibility had a significant influence on fear as hypothesized. This is generally consistent with earlier works involving the application of PMT to model the influence of fear appeal as a means of end user behavioural modification (Boss et al., 2015) ***The influence of fear on use of privacy settings was not significant*** in this study. It is interesting to note that in line with the research model, as well as the extended parallel-process model (Witte, 1994) and PMT (Rogers, 1983), fear 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 byproduct 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. This also supports the conclusions of Roskos-Ewoldsen et al. (2004) and de Hoog et al. (2005) that fear does not necessarily undermine the effectiveness of a threat appeal on the use of privacy settings. ***Sharing Benefits had a significant negative influence on adaptive response*****,** suggesting that users who find great enjoyment and satisfaction from sharing their location information on social networking sites are less inclined to make the adaptive change for protection. This finding is in line with expectations that the higher the rewards attained by not taking a recommended protective action, the less likely the individual is to take that action (Milne et al., 2000). According to a study conducted by Marett (2011) the hedonic nature of and the enjoyment gained from social networking is a stronger value for users than fear. Similar results occurred in a study on the use of privacy settings by adolescent on Facebook (Destici, 2015). The result showed that despite the users of Facebook being aware of the risks involved, they made the decision to put their personal information on their Facebook profile. Other studies showed that users avoid using privacy configuration settings on Facebook for an optimal experience of these social applications (Boyd & Ellison, 2007; Christofides et al., 2012; Peluchette & Karl, 2008). This study was able to show that social networking users may have noted the potential danger caused by posting one's location information online, but perhaps the enjoyment from being able to display that information is believed to be worth the risk and therefore do not make use of privacy settings. This is consistent with PMT.

4.4.2 **Coping Appraisal**

Self-efficacy is also important as a social network user must be confident and able to perform the necessary mitigation measures. This study highlights the importance of self-efficacy as well.

Self-efficacy had a strong impact on the use of privacy settings. These results imply that users will make more of an effort to apply privacy settings and thus experience high levels of confidence in doing so when their efforts are perceived as being effective and practicable. Not only did self-efficacy significantly influence the decision to adopt the recommended coping behaviour, but self-efficacy proved to be the second most powerful predictor of adaptive behaviour. This is consistent with PMT. Pahnila et al. (2007) also noted that self-efficacy was significant in explaining the use of IS security measures. The significant effect of self-efficacy represents that users would make use of privacy settings when they are confident in their ability to use it properly.

Overall, the results showed that self-efficacy plays an important and direct role in online protection behaviours. When users feel that they are faced with danger and are confident that they have the skills and ability to avoid or cope with the danger, they play an active role in securing their location information. The confidence that they can remove or reduce risk makes it more likely that they will choose adaptive behaviours. Having the confidence to take action reduces the feeling of being out of control and choosing avoidance behaviours may lead to secure online environment.

Other studies also show that self-efficacious individuals are more likely to protect their information and broader computing environment, and are less likely to take high-risk unprotected actions from being too trusting or lazy with respect to online protection (e.g. Kleinot & Rogers 1982; Rogers & Mewborn, 1976). These previous studies also support the positive interaction between self-efficacy and adoption of the recommended coping behaviour in this study. These studies found that increments in probability of occurrence resulted in higher behavioural intention scores only when they felt they were able to properly use privacy settings in preventing the threatened aversive outcome. The results of the present study revealed similar trends hence the fear appeal was effective.

This study's result did not confirm the hypothesis that the coping appraisal of response cost has a negative effect on the use of privacy settings. ***Response cost positively influenced the***

use of privacy settings meaning that users did not consider the inconvenience of using privacy settings a legitimate reason for not complying with safety measures. Although this is not consistent with PMT and our hypothesis, the direction of the relationship is consistent with prediction and findings elsewhere (Lee & Larsen, 2009; Workman et al., 2008). Similar studies (e.g. Herath & Rao, 2009a) that examined the effect of response cost on behavioural compliance presented a view comparable to the one being presented herein i.e. response cost did not negatively influence compliance intentions. A plausible reason for this result may be due to sample composition. For example, it is possible that while some participants may have positive view of the cost of implementing recommended security cautions; others may have differing perspectives on the issue. Workman et al. (2008) had asserted peoples' perception of this factor tend to vary. Nonetheless, a user's perception of the cost of use of privacy settings is a significant factor that positively influences the use of privacy settings in this area.

Hence, the results of the relationship between response cost and use of privacy settings suggests that negative outcome expectations, such as wasting a substantial amount of time or feeling frustrated when using privacy settings, does not have an impact on why people do not use privacy settings.

Response efficacy was found to positively influence the use of privacy settings; findings are consistent with those of several previous studies (Crossler & Belanger, 2010; Liang & Xue, 2010; Johnson, 2010; Johnson, 2015). The result showed that the response efficacy associated with using privacy settings was the most important predictor of using privacy settings, indicating that users are highly motivated to use privacy settings when they believe it would be effective in mitigating or preventing threat. Kleinot and Rogers (1982), and Rogers and Mewborn (1976) also support the positive interaction between response efficacy and adoption of the recommended coping behaviour in this study. These studies found that increments in probability of occurrence resulted in higher behavioural intention scores only when the coping response was considered effective in preventing the threatened aversive outcome. The results of the present study revealed similar trends hence the fear appeal was effective.

Maladaptive behaviour had a negative influence on the use of privacy settings. This is consistent with the hypotheses. This kind of behaviour prevents the users from protecting themselves. This behaviour involves a defensive resistance to fear appeal advising a user on

how to reduce the risk associated with posting their location information (Marett et al., 2011) and a belief that a threat is unavoidable no matter what is done by an individual (Rippetoe & Rogers, 1987). With this kind of belief, it was expected that maladaptive behaviour would have a negative influence on the use of privacy settings and the results supported the hypothesis.

5 CONCLUSION

5.1 Overview of Findings

The previous chapter involved the presentation of findings for this study and a discussion on these findings. This chapter is the concluding chapter for this dissertation and includes a response to the research question: How do fear appeals modify end-user behavioural intentions associated with the use of privacy settings in location-based social networks? Theoretical and practical implications, limitations and recommendation for future research are also included.

This dissertation investigated the factors that influence the use of privacy settings in SNS. Specifically, this research used the Protection Motivation Theory (PMT) as a theoretical lens to explain the effect perceived risk susceptibility, perceived risk severity, self-efficacy, response efficacy, privacy costs, sharing benefits and maladaptive behaviours have on the use of privacy settings by LBSN users after being issued with a fear appeal. It showed that fear appeals with more emphases on coping appraisal rather than threat appraisal can be used to motivate users to make use of privacy settings. Although not all the hypotheses were supported, the dissertation's objective was achieved. The results also showed evidence that PMT can be used to predict individual security behaviour.

The findings in this dissertation also illustrate the importance of knowing the risks faced along with the possible behaviours to protect from these risks. Implications of these findings were discussed along with avenues for future research.

This study is one of the few that used PMT in this specific context of the use of privacy settings on SNS. The results of the structural model testing indicate strong support for the research model. With the exceptions of H1 and H5, all other hypotheses were supported, indicating the research model has good explanatory power and implications for both researchers and practitioners. The downstream effect of the fear appeal treatment is evident in the significance of the paths linking risk susceptibility, response cost, response efficacy, self-efficacy with use of privacy settings. Interestingly, while both maladaptive hopelessness and maladaptive avoidance appear to have strong predictive ability, response cost has slightly more of an effect on behavioural intent. Finally, lack of support for H1 and H5, while not consistent with PMT, is consistent with the findings of numerous other studies

in which individual users perceive themselves to be less likely to experience a malicious attack than their peers (Loch et al., 1992; Schmidt & Arnett 2005). This study also proved that gender was not a significant factor in the intention to use privacy settings.

The findings of this study are generally consistent with earlier works involving the application of PMT to model the influence of fear appeal as a means of end user behavioural modification (Herath & Rao, 2009; Johnston & Warkentin, 2010). Other works involving PMT have posited competing outcomes, with little progress in the repeatability of findings (Bélanger & Crossler, 2011). Tests of the research model revealed consistent correlations among the conventional fear appeal elements and compliance intention, and threat severity and fear were not significant determinant in intentions to comply with recommended protective behaviour. The researcher highlights this outcome as evidence of the inadequacy of the fear appeal composition and the subsequent misspecification of PMT within the information security context. Fear appeal design and PMT do not distinguish between threats to the human asset and threats to information assets. Fear appeals modeled without this awareness will result in similar outcomes.

5.2 Contributions

This study contributes to the field of information systems by validating the relevance of a well-established theory for explaining human reaction to fear-inducing messages from the domain of social psychology to the domain of IS studies. PMT represents a culmination of years of research and improvements to fear appeal theory, and its impact within the realm of IS research, particularly information security, is promising. The research question investigated in this dissertation is of interest to social researchers who want to understand human behaviour related to information security. In addition, it is of interest to SNS administrators who are concerned with the everyday issue of keeping their platform secure. SNS administrators face the challenge of encouraging and motivating end user to practice security- related behaviour (Warkentin & Johnston, 2008) as research shows that the human factor is the weakest link in securing a computer system (Deloitte, 2007). 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. This study provides a

contribution in this respect and provides SNS administrators with insight for tailoring their fear appeals for maximum effectiveness. For example, response efficacy emerged as the most frequent determinant of the intention to use privacy settings. Therefore, focusing more on the coping appraisal rather than threat appraisal when designing fear appeal will help maximize the effectiveness and enhance the desired result. That is, our research indicates that properly worded communications will spur responses from users that are consistent with SNS goals with regard to the adoption of secure online behaviours.

The present study focused on the use of privacy settings. According to Straub and Welke (1998), individuals motivated to act securely in one phase of the security action cycle would similarly be motivated to engage in other safe behaviours. Accordingly, the results of this study support the use of fear-inducing arguments as an effective way to influence end user intentions to carry out recommended individual security actions. However, the findings indicate that these messages inspire different outcomes for different users based on their perceptions of efficacy, threat, benefits and cost. Users will react to fear inducing arguments in one of two ways: message rejection or message acceptance (Witte, 1992). Messages warning of new threats and advising a plan of action to counter the threat will inspire some users to accept the message and take appropriate action to reduce the threat. For others, their reaction may be to reject the message and to take action to reduce their fear (Witte, 1992), thereby leaving some threats unaddressed and exposing the user to potential harm. Therefore, a singular approach to this form of communication is not advised. Rather, to effectively wield fear as a motivator, SNS administrators must devise a strategy in which users are exposed to fear appeals with language suitable to their efficacy level.

Practitioners should note that a fear appeal is more than the knowledge of a threat, or merely scaring people; the existence of a statement that opposes insecure behaviour is not necessarily persuasive, nor does it necessarily invoke fear. A fear appeal requires a persuasive message that ideally is designed to heighten threat susceptibility sufficiently to generate fear and to help address maladaptive incentives to ignore the fear appeal. The fear appeal should likewise address issues that can increase self-efficacy and response efficacy while decreasing benefits. Hence, in practice, fear appeals typically require campaigns, interventions, and training. To increase their effectiveness, multiple applications over time are required. In summary, an effective fear appeal generally inspires

an adaptive approach to both threat appraisal and coping appraisal, resulting in an adaptive, protective response rather than message rejection.

This dissertation should provide SNS administrators with evidence for the need to use fear appeals and to present users with strong arguments for adhering to safe behaviour.

5.3 Limitations of this Study

When conducting research on a social phenomenon, such as individual security behaviours, decisions have to be made that impose limitations on the study. This study was done using previously validated instruments. The instruments were pilot tested, and subjected to reliability and validity measures. Statistical analyses on the data led to the elimination of outliers and incomplete responses. However, there were still limitations to this study which are discussed in this section.

This study measured a number of demographics about the respondents, including gender, age, and experience using SNS. The sample used in the present study wasn't broadly diverse in representing the South African online population; it was skewed toward young adults with high education levels compared to the general population. The result of the sample demonstrates a relative insensitivity to age and discipline. Because of this, the results of this study are not necessarily generalizable to other populations and caution should be used when trying to apply these findings to other groups of people.

One of the limitations inherent with self-reported data is social desirability bias or the tendency for respondents to complete surveys in a way that makes themselves look good to others (Mckenzie et al., 2002). Additionally, researchers in security have found that it is difficult to get good response rates from research that is as sensitive as security behaviours (Kotulic et al., 2004). In order to address these concerns, it is recommended that respondents are assured that their results are anonymous and to use a web-based data collection effort (Whitley, 2002). Following these recommendations, the data was collected utilizing online survey instruments. The results presented in this study are from those that chose to respond to the collection mechanisms used. There is likely a certain characteristic about those who chose not to respond that is lost using this approach. It is possible that those who are overly concerned about information security did not respond to the survey as they are predisposed not to share that information. Therefore, these findings are likely not

representative of those that are overly security conscious. One limitation of using online-based data collection efforts is the likelihood that those people who are not Internet savvy may not have completed this survey at all.

Although PMT is an intentions-focused model, it has been effectively extended to behaviours (Floyd et al., 2000). Actual behaviours are important for information security research because the end goal is to change security behaviours, not just security intentions. Examining the actual security behaviours instead of security intentions would have extended our understanding of security protection behaviours (Boss et al., 2015). An additional methodological benefit of measuring actual behaviours in addition to self-reported intentions and other measures is that such an approach greatly decreases the possibility of common-method biases by combining two methods for collecting data (Boss et al., 2015). Studies that focus solely on self-reports, as is the case with information security PMT literature, are subjected to greater threats from common-method bias (Podsakoff et al., 2003).

The cross-sectional timeline of this study should also be taken into consideration. The study was conducted based on the current situation and state of the surveyed social networking sites users, therefore the factors that impact their intention to use location privacy settings may change over time. Cross-sectional surveys also do not conclusively establish causality. This study measured independent and dependent variables at the same time. To be able to conclude that independent variables predict the dependent variable, they should be measured at the prior time point to the dependent variable.

The method used in determining the intention to use location privacy settings was based on the perception of respondents and there was no confirmatory test carried out to verify these strategies beyond the surveyed respondents.

Another limitation is the use of only one context in the studies: the use of privacy settings in SNS. Examining other contexts of behavioural security would have helped to further establish the efficacy of PMT based research and identify additional areas for improvement.

5.4 Suggestion for future research

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). Therefore, 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, 1994; Witte & Allen, 2000). For example, future research could explore antecedents for why individuals fail to behave in a secure manner.

There is need for further methodological and theoretical research to refine fear appeals and fear measurement for information security. For one, creating ideal fear appeals is not easy, because they should be built in view of the threat (severity and susceptibility) and in view of efficacy (self-efficacy and response efficacy), and they need to be generalizable to a wide target audience to create an appropriate level of fear (Boss et al., 2015). Also, as demonstrated by Johnston et al. (2015), they need to have personal relevance. Thus, more work is needed to establish guidelines on how to inspire the right level of fear and to explain better what happens if too much fear is generated. It is also likely that there are behavioural security situations for which PMT and fear appeals simply are not appropriate and for which other theoretical approaches may be better. More can be done to ensure that adaptive threat appraisal and coping-appraisal responses are generated with fear appeals and to better consider ways to also increase efficacy as part of fear appeals.

The researcher also expects that there are key differences in longitudinal and one-time fear-appeal studies that require further theoretical and methodological study. The researchcer attributes this to the difference between a strong and focused one-time fear-appeal message and one that is made somewhat weaker by the longitudinal nature of the manipulation

Security researchers might find it unrealistic to measure maladaptive response if the behaviour is not focused on a single moment or decision. Future researchers might ask participants in longitudinal field studies to recall their fear or perceptions of maladaptive responses after the study's completion as a surrogate for assessment during the study. Such measurement can be particularly valuable in cases in which fear appeals differ greatly in effectiveness or in which individual differences lead participants to perceive them differentially. The researcher thus believes that the timing of fear appeals and of fear

measurement and the design and process of fear-appeal delivery are highly relevant to the IT artifact delivery, design, and process in security research. The researcher leaves it to future research to expand and improve on this vast area of opportunity in IT artifact-related fear appeals.

More research needs to be performed with even older participants or those in other occupations for greater assurance of the invariability of results. Future research should also explore the relationships conceptualized in our study using a stratified random sample representative of South African population as well as populations from other countries (Belanger & Crossler, 2011). The relationship between culture and the use of privacy settings on SNS could be a very interesting direction to research.

6 REFERENCES

Acquisti, A., Gross, R., & Stutzman, F. (2011). Faces of Facebook: Privacy in the age of augmented reality (pp. 1-68). Retrieved from http://marchiondelli.com/Blog/wp-content/uploads/2013/10/acquisti-face-BH-Webinar-2012-out.pdf

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613-643.

Arthur, D., & Quester, P. (2004). Who's afraid of that ad? Applying segmentation to the protection motivation model. *Psychology & Marketing*, *21*(9), 671-696.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, *16*(1), 74-94.

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

Bhattacherjee, A. (2012). *Social Science Research: Principles, Methods, and Practices*. 2nd Edition, 1 – 158. Creative Commons Attribution.

Block, L. G., & Keller, P. A. (1995). When to accentuate the negative: The effects of perceived efficacy and message framing on intentions to perform a health-related behavior. *Journal of Marketing Research*, 192-203.

Bollen, K. A. (1989). A new incremental fit index for general structural equation models. *Sociological Methods & Research*, *17*(3), 303-316.

Bollen, K. A., & Lennox, R. (1991). Conventional Wisdom on Measurement: A Structural Equation Perspective. *Psychological Bulletin* 110(2), pp. 305-314.

Borena, B., Belanger, F., & Ejigu, D. (2013). Social networks and information privacy: A model for low-income countries. *Americas Conference on Information Systems 2013, Illinois, USA.*

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & 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.

Boyd, D., & Ellison, NB. (2007). *Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication*, *13*(1), 11.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548.

Burrell, G., & Morgan, G. (1979). *Sociological paradigms and organizational analysis* (Vol. 248). London: Heinemann.

Carlson, R. D., & Grabowski, B. L. (1992). The Effects of Computer Self-Efficacy on Direction-Following Behavior in Computer Assisted Instruction. *Journal of Computer-Based Instruction*, *19*(1), 6-11.

Chenoweth, T., Minch, R., & Gattiker, T. (2009, January). Application of protection motivation theory to adoption of protective technologies. In *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on* (pp. 1-10). IEEE.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern methods for business research*, *295*(2), 295-336.

Choobineh, J., Dhillon, G., Grimaila, M. R., & Rees, J. (2007). Management of information security: Challenges and research directions. *Communications of the Association for Information Systems*, *20*(1), 57.

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.

Chung, S. H., Schwager, P. H., & Turner, D. E. (2002). An empirical study of students' computer self-efficacy: Differences among four academic disciplines at a large university. *Journal of Computer Information Systems*, *42*(4), 1-6.

Clark, L. A., & Watson, D. (1995). Constructing validity: Basic issues in objective scale development. *Psychological Assessment*, *7*(3), 309.

Comparatives, A. V. (2013). IT Security survey 2013. *Rapport Technique, AV Compara*.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, 19(2), 189-211.

Compeau, D., Higgins, C. A., & Huff, S. (1999). Social cognitive theory and individual reactions to computing technology: A longitudinal study. *MIS Quarterly*, 23(2), 145-158.

Creswell, J. W. (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (3rd ed.). Thousand Oaks: Sage Publications, Inc.

Criddle, L. (2006). *Look Both Ways: Help Protect Your Family on the Internet*. Redmond, WA: Microsoft Press.

Croog, S. H., & Richards, N. P. (1977). Health beliefs and smoking patterns in heart patients and their wives: a longitudinal study. *American Journal of Public Health*, *67*(10), 921-930.

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

Crossler, R., & Bélanger, F. (2014). An extended perspective on individual security behaviors: Protection Motivation Theory and a Unified Security Practices (USP) instrument. *ACM SIGMIS Database*, *45*(4), 51-71.

Deloitte, T. (2007). Tohmatsu. (2003). *Deloitte Sustainability Reporting Scorecard*.

Destici, A. (2015). *Determining the factors that influence the use of privacy configuration settings on Facebook: an empirical study among adolescents* (Master's Thesis, University of Twente).

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, *11*(2), 127-153.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, *8*(7), 386.

Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210-230.

Hair Jr, J., Sarstedt, M., Hopkins, L., & G. Kuppelwieser, V. (2014). Partial least squares structural equation modeling (PLS-SEM) An emerging tool in business research. *European Business Review*, *26*(2), 106-121.

Fagan, M. H., Neill, S., & Wooldridge, B. R. (2004). An empirical investigation into the relationship between computer self-efficacy, anxiety, experience, support and usage. *Journal of Computer Information Systems*, *44*(2), 95-104.

Farrell, A. M. (2010). Insufficient discriminant validity: A comment on Bove, Pervan, Beatty, and Shiu (2009). *Journal of Business Research*, *63*(3), 324-327.

Fenech, T. (1998). Using perceived ease of use and perceived usefulness to predict acceptance of the World Wide Web. *Computer Networks and ISDN Systems*, *30*(1-7), 629-630.

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.

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equations with Unobservable Variables and Measurement Error. *Journal of Marketing Research* 18(1), 39-50.

Fry, R., & Prentice-Dunn, S. (2005). Effects of Coping Information and Value Affirmation on Responses to Perceived Health Threat. *Health Communication* 17(2), 133-147.

Gefen, D., & Straub, D. W. (2005). A Practical Guide to Factorial Validity using PLS-Graph: Tutorial and Annotated Example. *Communications of the AIS* 16(25), 91-109.

Ghorab, K. E. (1997). The impact of technology acceptance considerations on system usage, and adopted level of technological sophistication: An empirical investigation. *International Journal of Information Management*, *17*(4), 249-259.

Grothmann, T., & Reusswig, H. (2006). People at Risk of Flooding: Why Some Residents Take Precautionary Action while Others Do Not. *Natural Hazards* (38), 101-120.

Hair, J. F. (2006): Multivariate Data Analysis. *Auflage, Upper Saddle River*.

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2014). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). *SAGE Publications.*

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed, a silver bullet. *Journal of Marketing Theory and Practice*, 19(2), 139-152.

Hair, J. F., Ringle, C. M., & 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. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the Academy of Marketing Science*, 40(3), 414-433.

Hanisch, K. A., Hulin, C. L., & 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.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115-135.

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. *In New Challenges to International Marketing*, 277-319. Emerald Group Publishing Limited.

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

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

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. *Information Systems Journal*, *24*(1), 61-84.

Hoffer, J. A., & Straub, D. W. (1989). The 9 to 5 Underground: Are You Policing Computer Crimes? *Sloan Management Review* 30(4), 35-43.

Hoog, N. D., Stroebe, W., & Wit, J. B. (2005). The Impact of Fear Appeals on Processing and Acceptance of Action Recommendations. *Personality and Social Psychology Bulletin* 31(1), 24-33.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, *54*(6), 54-60.

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

Interactive, H. (2010). GLSEN. (2005). *From teasing to torment: School climate in America, a survey of students and teachers*, 499-1.

Johnson, R. D., & Marakas, G. M. (2000). Research report: the role of behavioral modeling in computer skills acquisition: toward refinement of the model. *Information Systems Research*, *11*(4), 402-417.

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

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, *53*(1), 59-68.

Kleinot, M. C., & Rogers, R. W. (1982). Identifying effective components of alcohol misuse prevention programs. *Journal of Studies on Alcohol*, *43*(7), 802-811.

Kline, R. B. (2011). Convergence of structural equation modeling and multilevel modeling. *NA*.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management*, *41*(5), 597-607.

Kumar, K., & Lu, Y. H. (2010). Cloud computing for mobile users: Can offloading computation save energy? *Computer*, *43*(4), 51-56.

Lam, J. C., & Lee, M. K. (2006). Digital inclusiveness: Longitudinal study of Internet adoption by older adults. *Journal of Management Information Systems*, *22*(4), 177-206.

Lampe, C., Wash, R., Velasquez, A., & Ozkaya, E. (2010, April). Motivations to participate in online communities. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1927-1936). Georgia, USA.

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, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology*, *27*(5), 445-454.

Lee, W., Fan, W., Miller, M., Stolfo, S. J., & Zadok, E. (2002). Toward cost-sensitive modeling for intrusion detection and response. *Journal of Computer Security*, *10*(1-2), 5-22.

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

Lee, Y., Kozar, K. A., & Larsen, K. R. (2003). The technology acceptance model: Past, present, and future. *Communications of the Association for information systems*, *12*(1), 50.

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

Levin, R. C., Cohen, W. M., & Mowery, D. C. (1985). R & D appropriability, opportunity, and market structure: new evidence on some Schumpeterian hypotheses. *The American Economic Review*, *75*(2), 20-24.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394.

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

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly*, 16(2), 173-186.

Loch, K. D., Straub, D. W., & Kamel, S. Kamel. (2003). Diffusing the Internet in the Arab World: The Role of Social Norms and Technological Culturation. *IEEE Transactions on Engineering Management* 50(1), 45-63.

Lowry, P. B., & Gaskin, J. (2014). Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE Transactions on Professional Communication*, *57*(2), 123-146.

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies. *Information Systems Journal*, *25*(5), 433-463.

Maddux, J. E. (1993). Social cognitive models of health and exercise behavior: An introduction and review of conceptual issues. *Journal of Applied Sport Psychology*, *5*(2), 116-140.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469-479.

Malhotra, M. K., & Grover, V. (1998). An assessment of survey research in POM: from constructs to theory. *Journal of Operations Management*, *16*(4), 407-425.

Marcoulides, G. A., & Saunders, C. (2006). Editor's comments: PLS: a silver bullet? *MIS Quarterly*,30(2), 3-9.

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

Maximilien, E. M., Grandison, T., Liu, K., Sun, T., Richardson, D., & Guo, S. (2009). Enabling privacy as a fundamental construct for social networks. In *Computational Science and Engineering. CSE'09.* (4), 1015-1020.

McClendon, B., & Prentice-Dunn, S. (2001). Reducing Skin Cancer Risk: An Intervention Based on Protection Motivation Theory. *Journal of Health Psychology* 6 (3), 321-328.

McKenzie, K., Whitley, R., & Weich, S. (2002). Social capital and mental health. *The British Journal of Psychiatry,* 181(4), 280-283.

McMath, B. F., & Prentice-Dunn, S. (2005). Protection Motivation Theory and Skin Cancer Risk: The Role of Individual Differences in Responses to Persuasive Appeals. *Journal of Applied Social Psychology,* 35(3), 621-643.

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.

Mingers, J. (2001). Combining IS Research Methods: Towards a Pluralist Methodology. Information Systems Research, 12(3), 240-259.

Mitchell, K., Finkelhor, D., & Wolak, J. (2001). Risk Factors for and Impact of Online Sexual Solicitation of Youth. *Journal of the American Medical Association* 285(23), 3011-3015.

Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, *28*(6), 2366-2375.

Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research*, *2*(3), 192-222.

Mulilis, J. P., & Lippa, R. (1990). Behavioral change in earthquake preparedness due to negative threat appeals: A test of protection motivation theory. *Journal of Applied Social Psychology*, *20*(8), 619-638.

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.

McIntosh, Zajonc, Peter S., Vig, Stephen W., & Emerick, D. (1997). Facial movement, breathing, temperature, and affect: Implications of the vascular theory of emotional efference. *Cognition & Emotion*, *11*(2), 171-196.

Neuman, & W. Lawrence. (1994). *Social research methods: Qualitative and quantitative approaches (2nd Edition ed.).* Boston: Allyn and Bacon.

Ng, B., Kankanhalli, A., & Y. Xu. (2009). Studying Users' Computer Security Behaviour: A Health Belief Perspective. *Decision Support Systems* 46(4), 815-825.

Nunnally, J., & Bernstein, I. (1994). Psychometric theory. New York, NY: McGraw Hill.

O'Keefe, D. J. (1990). Persuasion: Theory and Research, Newbury Park, CA: Sage Publications.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying Information Technology in Organizations: Research Approaches and Assumptions. *Institute for Operations Research and the Management Sciences*, *2*(1), 1–28. Retrieved from http://www.jstor.org/stable/23010611

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

Pahnila, S., Siponen, M.A., & Mahmood, M. (2007). Employees' Behaviour towards IS Security Policy Compliance. *Proceedings of the 40th Hawaii International Conference on System Sciences, Waikoloa HI*.

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.

Peluchette, J., & Karl, K. (2008). Social networking profiles: An examination of student attitudes regarding use and appropriateness of content. *Cyber Psychology & Behavior*, *11*(1), 95-97.

Petter S., Straub, D. W., & Rai, A. (2007). Specifying Formative Constructs in Information Systems Research. *MIS Quarterly* 31(4), 623-656.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879.

Posey, C., Bennett, B., Roberts, T., & Lowry, P. B. (2011). When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse. *Journal of Information System Security*, 7(1), 24-47.

Rainie, L., Smith, A., & Duggan, M. (2013). Coming and going on Facebook. *Pew Research Center's Internet and American Life Project*. Retrieved from http://pewinternet.org/Reports/2013/Coming-and-going-on-facebook.aspx

Reardon, J. L., & Davidson, E. (2007). An organizational learning perspective on the assimilation of electronic medical records among small physician practices. *European Journal of Information Systems*, *16*(6), 681-694.

Rifon, N. J., LaRose, R., & Choi, S. (2005). Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. *Journal of Consumer Affairs*, *39*(2), 339-362.

Ringle, C. M., Wende, S., & Will, A. (2005). SmartPLS 3.0 (beta).

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. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *Journal of Psychology* (91), 93-114.

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

Rogers, R. W., & Mewborn, C. R. (1976). Fear appeals and attitude change: effects of a threat's noxiousness, probability of occurrence, and the efficacy of coping responses. *Journal of Personality and Social Psychology*, *34*(1), 54.

Rogers, R., & Prentice-Dunn, S. (1997). Protection Motivation Theory, in D. S. Gochman (Ed.) *Handbook of Health Behaviour Research: Vol.1. Determinants of Health Behaviour: Personal and Social*, New York, NY: Plenum.

Roskos-Ewoldsen, D. R., Yu, H. J., & Rhodes, N. (2004). Fear Appeal Messages Affect Accessibility of Attitudes Toward the Threat and Adaptive Behaviours. *Communication Monographs* 71(1), 49-69.

Saeri, A. K., Ogilvie, C., La Macchia, S. T., Smith, J. R., & Louis, W. R. (2014). Predicting Facebook users' online privacy protection: Risk, trust, norm focus theory, and the theory of planned behavior. *The Journal of social psychology*, *154*(4), 352-369.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students (5th Edition ed.).* London: Pearson Education/Prentice Hall.

Schmidt, M. B., & Arnett, K. P. (2005). Spyware: a little knowledge is a wonderful thing. *Communications of the ACM*, *48*(8), 67-70.

Sekaran, U. (2003). *Research methods for business: A skill building approach* (4th ed.). New York: John Wiley.

Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, *48*, 199-207.

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

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

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

Sonmez, S., & Graefe, A. (1998). Determining Future Travel Behaviour from Past Travel Experience and Perceptions of Risk and Safety. *Journal of Travel Research* 37(2), 171-178.

Stephens, P. (2005). A decision support system for computer literacy training at universities. *Journal of Computer Information Systems*, *46*(2), 33-44.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, 22(4), 441-469.

Straub, D. W., Boudreau, M. C., & Gefen, D. (2004). Validation Guidelines for IS Positivist Research. *Communications of the Association for Information Systems,* 13(1), 63.

Tanner, J., Hunt, J. & Eppright, D. (1991). The Protection Motivation Model: A Normative Model of Fear Appeals. *Journal of Marketing,* 55(3), 36-45.

Tsai, H., Compeau, D. & Haggerty, N. (2007). Of Races to Run and Battles to be Won: Technical Skill Updating, Stress, and Coping of IT Professionals. *Human Resource Management* 46(3), 395-409.

Tschersich, M., & Botha, R. (2014). Exploring the impact of restrictive default privacy settings on the privacy calculus on social network sites. Paper presented at the *European Conference on Information Systems 2014, 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.

Van De Garde-Perik, E., Markopoulos, P., De Ruyter, B., Eggen, B., & Ijsselsteijn, W. (2008). Investigating privacy attitudes and behavior in relation to personalization. *Social Science Computer Review*, *26*(1), 20-43.

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, *29*(4), 263-290.

Venkatesh, V., Davis, F. D., & Morris, M. G. (2007). Dead or alive? The development, trajectory and future of technology adoption research. *Journal of the Association for Information Systems*, *8*(4), 267.

Whitley, E., & Ball, J. (2002). Statistics review 4: sample size calculations. *Critical Care*, *6*(4), 335.

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

Witte, K. (1994). Fear control and danger control: A test of the extended parallel process model (EPPM). *Communications Monographs*, *61*(2), 113-134.

Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior*, *27*(5), 591-615.

Wold, S., Martens, H., & Wold, H. (1983). The multivariate calibration problem in chemistry solved by the PLS method. *In Matrix pencils* (286-293). Springer Berlin Heidelberg.

Wong, K. K. K. (2013). Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin*, *24*(1), 1-32.

Woon, I., Tan, G. W., & Low, R. (2005). A protection motivation theory approach to home wireless security. *ICIS 2005 Proceedings*, 31.

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.

Wu, J. H., & Wang, S. C. (2005). What drives mobile commerce? An empirical evaluation of the revised technology acceptance model. *Information & Management*, *42*(5), 719-729.

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

Appendix A – Survey Approval letter

Faculty of Commerce

Private Bag X3, Rondebosch, 7701
2.26 Leslie Commerce Building, Upper Campus
Tel: +27 (0) 21 650 4375/ 5748 Fax: +27 (0) 21 650 4369 E-mail: com-faculty@uct.ac.za
Internet: www.uct.ac.za
@Commerce_UCT **UCT Commerce Faculty Office**

21 April 2016 Ref:14042011

Henry Oladimeji

Project title: Factors influencing the use of privacy settings in Location-Based Social Networks

Dear Researcher,

This letter serves to confirm that this project as described in your submitted protocol has been approved. You will need to obtain permission from the Executive Director, Department of student Affairs before you commence data collection.

Please note that if you make any substantial change in your research procedure that could affect the experiences of the participants, you must submit a revised protocol to the Committee for approval.

Regards,

Ms. Samantha Alexander
Administrative Assistant
University of Cape Town
Commerce Faculty Office
Room 2.24 | Leslie Commerce Building

Office Telephone: +27 (0)21 650 2695
Office Fax: +27 (0)21 650 4369
E-mail: samantha.alexander@uct.ac.za
Website: www.commerce.uct.ac.za<http://www.commerce.uct.ac.za/>

Appendix B – Survey Introduction Letter

Department of Information Systems
Leslie Commerce Building
Engineering Mall, Upper Campus
OR
Private Bag. Rondebosch 7701
Tel: +27 (0) 21 650 4028 Fax: +27 (0) 21650 2280
Internet: http://www.commerce.uct.ac.za/informationsystems/

February 2016

Dear Sir/Madam,

I am a student enrolled in the Masters programme in the Department of Information Systems at the University of Cape Town. As part of the course curriculum I am required to complete a research project. The research embarked by me, in this study is titled*: Individual use of location privacy settings in social network: a fear appeal approach*. This research project has been approved by the Commerce Faculty Ethics in Research Committee. The main purpose of this research is to examine the use of location privacy settings in social networks. The motivation behind this study lies in the fact that location-based information is a common part of social networks, and can be misused by third parties if not protected. Finding how individuals protect their location information in social networks is therefore of paramount importance. Your participation in this research will be greatly appreciated.

Your participation in this research is voluntary. You can choose to withdraw from the research at any time. The questionnaire will take approximately 20 minutes to complete. You will not be requested to supply any identifiable information, ensuring anonymity of your responses. All information will be treated as confidential and used solely for the purpose of this study.

The findings of this research will be compiled in a report that will be presented to the University of Cape Town for academic purposes. Also, on request, a copy of this research will be made available to participants. Should you have any questions regarding the research please feel free to contact the researcher (oldhen003@myuct.ac.za). By participating in the survey you agree to the above points.

Thank you for your time and participation.

Sincerely,

Signed by candidate

Signature Removed

Signed by candidate

Signature Removed

Oladimeji Henry
Masters Student
Department of Information Systems
University of Cape Town
Email: oldhen003@myuct.ac.za

Dr. Jacques Ophoff
Research Supervisor
Department of Information Systems
University of Cape Town
Email: jacques.ophoff@uct.ac.za

Appendix C – Fear Appeal

You should be aware of potential online dangers on location based social networking websites and what kind of threats they can present. The following are reported cases:

A security guard in South Africa targeted a woman he met on a LBSN who had earlier rejected his romantic advances. The innocent woman wasn't aware that her location information was visible to everyone on her friend list. The security man took advantage of her location information by stalking her and posting her home address on Internet forums and websites. The victim received several unsolicited visits from strangers at her residence. The security guard was sentenced to six years in prison.

In May of 2012, Foursquare turned over the names of 245 registered sex offenders who were using their site to meet, stalk and rape vulnerable underage girls who had their location information visible to the FBI.

From The Washington Post: The FBI last month warned Facebook users of a phony bulletin post urging people to click on a link to meet interesting people around your vicinity. Early last month, unsolicited instant messages attempted to lure MySpace users into divulging location information.

From The Mirror: Lara Coton knows about the dangers of putting location tagged photos on the net. The 17-year-old submitted innocent tagged photographs of their family on vacation. By doing so, people on her friends list knew they were away and the house was empty so they used the opportunity and the privileged information to rob the victim's house. She was horrified to discover that the information she gave out led to her family house been robbed.

You should also be aware of potential online dangers on social networking websites and how likely they are to occur. The following are statistics from the book Look Both Ways by Linda Criddle and from other websites:

Two in five individuals are sexually solicited online and one in five have their location information visible leading to physical violence such as stalking and rape every year in the United States, and a similar number is estimated in other countries.

Contrary to common belief, not all online victims are female. 25 percent of reported victims are male.

23 percent of online victims of sex crimes and stalking were between the ages of 18 to 25. A recent study shows that forty percent of the respondents had been threatened due to the carelessness of making their location information visible on social networking sites. (Paul Bocij, firstmonday.com).

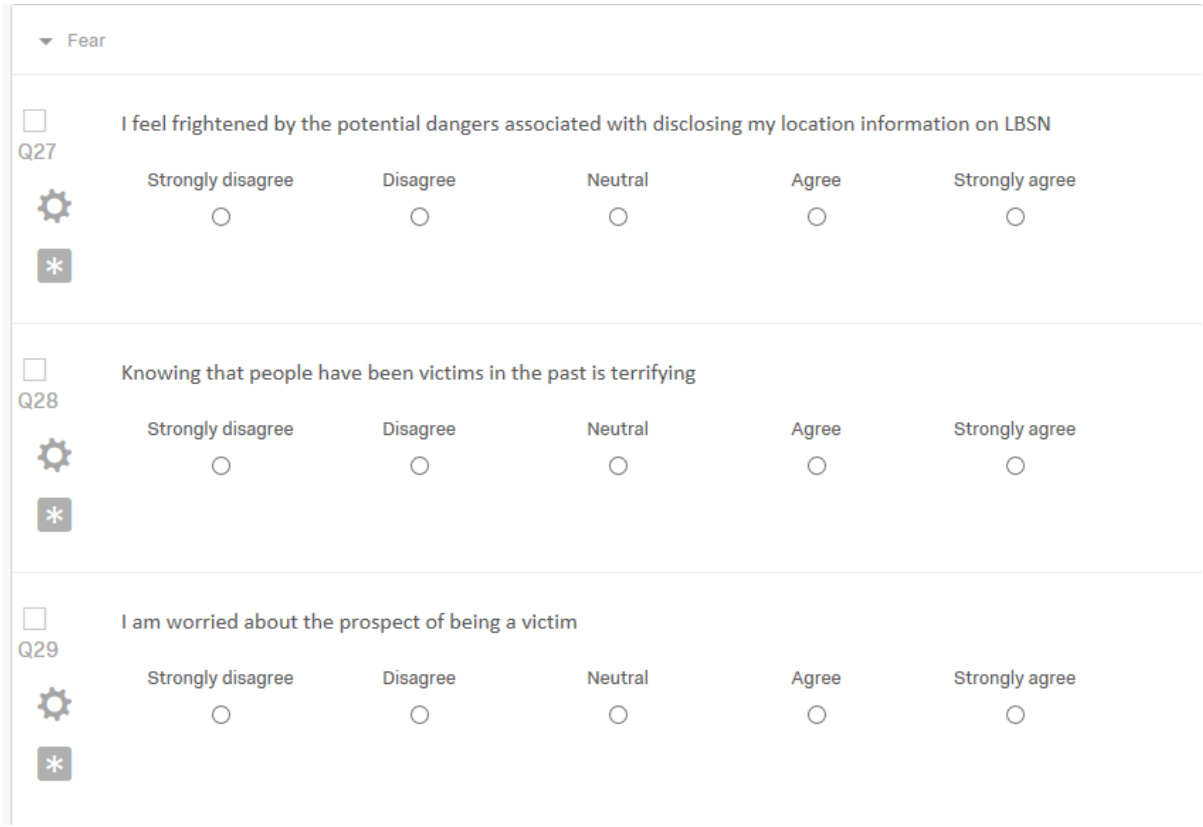
Finally, you should also be aware of possible ways to protect yourself and your location information when using social networking websites, whether you maintain a profile or you post messages on others' profiles. The following are some safety tips from the website Cybertipline.com:

Check the privacy settings of the social networking sites that you use:

- Set privacy so that people can only be added as your friend if you approve it.
- Set privacy so that people can only view your profile if you have approved them as a friend.
- Set privacy to switch off your location information visibility and if for any reason you have to reveal your location information make sure only family and friends you trust have access to this information.

Remember that posting location information about your friends could put them at risk. Protect your friends by not posting any names and location information. Refrain from making or posting plans, activities and travels on your site.

Appendix D – Questionnaire



Risk Severity

Q1 In general, it is risky to disclose my location information on a LBSN.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
○	○	○	○	○

Q2 There would be high potential for loss associated with posting my location information on LBSN.

Strongly Disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Q3 It is uncertain who might have access to my location information on LBSN.

Strongly Disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Q4 Posting my location information on LBSN would involve many unexpected problems.

Strongly Agree	Agree	Neutral	Disagree	Strongly disagree
○	○	○	○	○

Risk susceptibility

Q5 My privacy is at risk when disclosing location information

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Q6 It is possible that I become a victim

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Q7 It is likely that I become a victim

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Benefits

Q8 I enjoy sharing my location information with others

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Q9 Sharing my location information with others is fun to do.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Q10 Sharing my location information with others is a boring activity.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Q11 Sharing my location information with others does not hold my attention at all.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Q12 I would describe sharing my location information with others as interesting.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Q13 I think sharing my location information with others is quite enjoyable.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Q14 I earn respect from others by sharing my location information with them.

Strongly Disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Q15 I feel sharing my location information with others improves my status within my group of friends.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Q16 I share my location information with others to improve my reputation.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

Self-efficacy

Q17 I have the ability to use privacy settings without much effort.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Q18 Privacy settings is easy to use.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Q19 Privacy settings is convenient to use

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Response Efficacy

Q20 Using privacy settings works for protection

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Q21 Privacy settings is effective for protection

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Q22 When using privacy settings my location information is more likely to be protected

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Response Cost

Q23 Using privacy settings would require a considerable amount of effort other than time

Strongly disagree	Somewhat disagree	Neutral	Somewhat agree	Strongly agree
○	○	○	○	○

Q24 There is too much work associated with trying to increase my information protection through the use of privacy settings.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Q25 Using privacy settings would be time consuming.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Adaptive Response: Intention to use privacy settings

Q30 In future I intend using privacy settings to control access to my location information

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Q31 In future I predict using privacy settings

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Q32 In future I plan on using privacy settings

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Maladaptive Response: Avoidance

Q33 I try not to think about the potential danger of not using my privacy settings.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Q34 I am not at risk from the potential danger of posting my location information on LBSN

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Q35 Not using privacy settings save me time

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Maladaptive Response: Hopelessness

Q36 There is nothing I can do to avoid the potential dangers associated with disclosing my location information on LBSN.

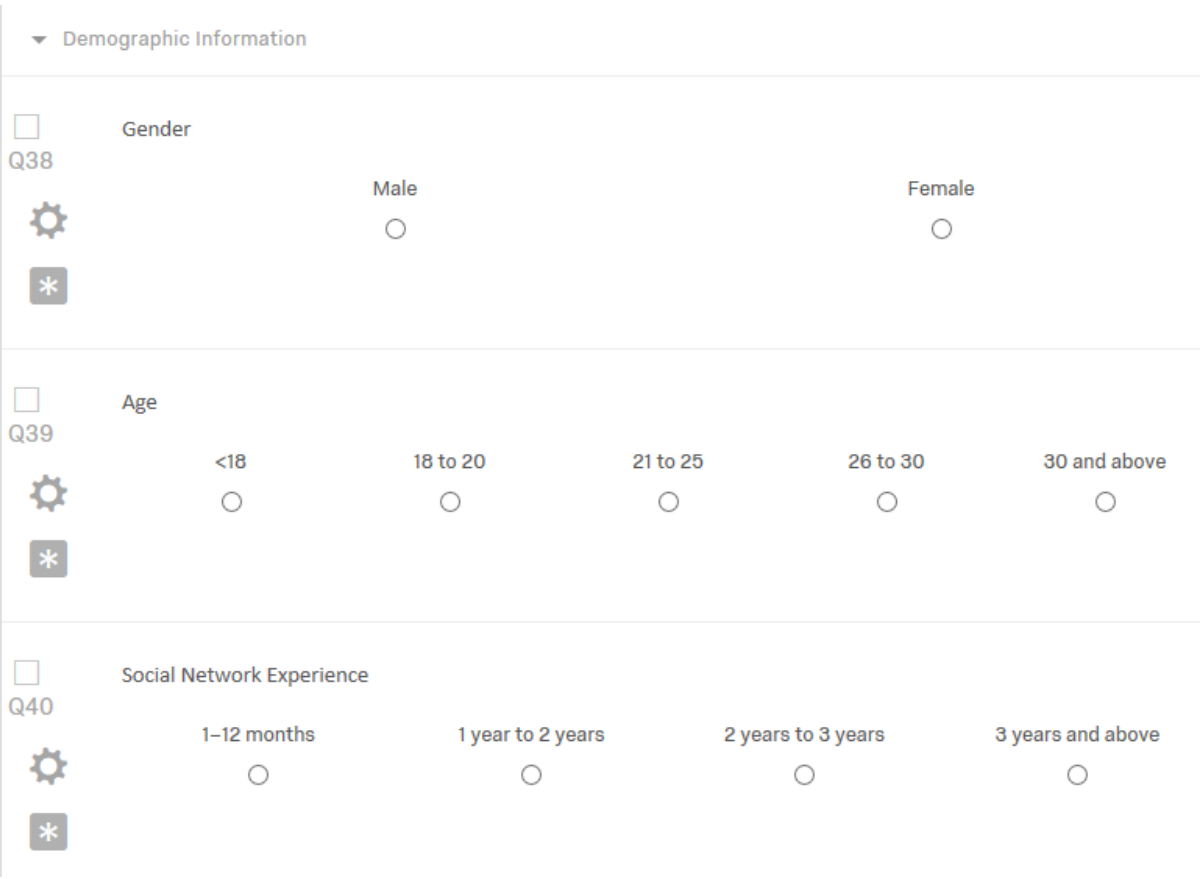
Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Q37 I feel it is useless to use privacy settings to protect myself from the potential dangers associated with LBSN.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○

Q38 I am at a loss as to how to use privacy settings to protect myself from the potential dangers associated with LBSN

Strongly disagree	Disagree	Neutral	Agree	Strongly agree
○	○	○	○	○


Demographic Information
Q38
Gender
Male
Female
Q39
Age
<18
18 to 20
21 to 25
26 to 30
30 and above
Q40
Social Network Experience
1–12 months
1 year to 2 years
2 years to 3 years
3 years and above