2017

Emergency Notification on Mobile Devices – A Trade-off between Protection Motivation and Privacy Concern

Jing Zhang
University of Canterbury, jzh115@uclive.ac.nz

Annette Mills
University of Canterbury, annette.mills@canterbury.ac.nz

Nelly Todorova
University of Canterbury, nelly.todorova@canterbury.ac.nz

Emergency Notification on Mobile Devices – A Trade-off between Protection Motivation and Privacy Concern

Jing Zhang
UC School of Business
University of Canterbury
Christchurch, New Zealand
Email: jzh115@uclive.ac.nz

Annette Mills
UC School of Business
University of Canterbury
Christchurch, New Zealand
Email: annette.mills@canterbury.ac.nz

Nelly Todorova
UC School of Business
University of Canterbury
Christchurch, New Zealand
Email: nelly.todorova@canterbury.ac.nz

Abstract

Worldwide, natural disasters are increasing. In 2016 alone there was over $175 billion in damages and 8900 lives lost. To mitigate the impact of these events on people, countries are turning to location-based mobile emergency alert systems (MEAS) for their practical benefits and ability to deliver personalised emergency notifications to individuals. Most systems depend on persons choosing to use the service and share personal details. However concerns about data privacy have been raised. Focusing people's desire to protect themselves from harm, this paper draws on Protection Motivation Theory and work on privacy concern to evaluate willingness to use MEAS, which require the disclosure of personal information to service providers. Results using data from 103 respondents are reported. The findings enhance understanding of MEAS use, and provide insights to service providers and government agencies for implementing MEAS.

Keywords: emergency alert systems, protection motivation theory, privacy concern

1 INTRODUCTION

Natural disasters are increasingly common. The number of natural disasters worldwide has increased by more than four times in the last few decades (Gutierrez, 2008). These adverse events can have natural or human causes and include earthquakes, tsunamis, floods and fires. These events can cause loss of human lives and economic damage. Their average economic impact has increased from US$14 billion in 1976-1985 to US$140 billion in 2005-2014, with the number of persons affected rising from 60 million to over 170 million for the same periods (GFDRR, 2016). All countries are affected directly or indirectly by disasters leading to significant challenges for governments and local authorities.

Disaster and emergency management aims to minimize the impact of natural disasters. National and local government bodies work towards development and implementation of frameworks and tools to improve prevention, protection, preparedness, and response to such events. (Alfieri et al. 2012). Preparedness as a component of disaster management refers to informing citizens about risks and what to do in the event of emergency. Early warning and emergency alert systems disseminate information on developing emergency situations at the individual, organizational and national level. Traditional emergency alert approaches such as sirens, radio, television, and landlines can only reach a limited number of people. For disasters that require immediate protective actions, these approaches may miss potential targets who do not have immediate access to these media. As the mobile connection rate is incredibly high and continuously growing (e.g. the number of mobile phones in use is exceeding the population in many countries such as China, New Zealand, etc. (www.statista.com), using mobiles for emergency notification purposes becomes an ideal option for most countries for their emergency management. A location-based Mobile Emergency Alert Service (MEAS) provides prompt emergency alerts via mobile devices based on user's current location and personal profile. MEAS have saved lives and properties in many cases (http://www.nws.noaa.gov).

Similar to other location-based services, MEAS provide messages that are tailored to the individual preferences based on their location. They require users to register and disclose personal information (e.g. location information, name, address, medical information) to receive customized notifications. Therefore, users would be exposed to the potential risks that raise privacy concerns. Consideration of the general acceptance and concerns of individuals such as the use of their personal information is an open issue, impacting the design and implementation of such systems. Some systems initially provide notifications without the users' consent, and allow users to opt-out of receiving the notifications. For example, in Australia following the Black Sunday bushfires (Feb 7, 2009) which claimed 173 lives, the government quickly legislated the declaration of an emergency as an amendment to the Privacy Act 1988, giving government agencies and emergency services access to telecommunications details, such as name, address and phone number (whether listed or unlisted) which can be used during an emergency to deliver personalized information to the receiver including warning information and specific directions. However, alerts for most systems are only issued to users who have registered or subscribed to the service. However, the uptake of opt-in can be slow as evidenced in New Zealand, a country that is frequently threatened by natural disasters such as earthquakes and flash flooding; yet only around 35,000 people are subscribed to Auckland's Civil Defence app representing only 2.4% of the local population (Auckland Council, 2016).

For MEAS to be effective, the potential receiver must be willing to disclose their mobile device location data and other personal information to the notification provider. In other words, the more personalised the notification that the user would like to receive, the more personal information (such as location, demographics, status of health) the individual needs to disclose. This leads to the issue that people may not be willing to disclose their personal information, and to give up some of their privacy in exchange for customized services (Kim and Lee, 2009). When personal information is required by an online service, concerns are usually raised about the potential misuse of the information (Zhao, 2012). This argument is supported by a prior study (Xu et al. 2009) that revealed that users of location-based services are reluctant to disclose personal information when they believe there is a high potential of privacy invasion or a lack of effective protection of their personal information. General privacy concern, as "an individual's general tendency to worry about information privacy" (Malhotra et al. 2004), is believed to play a vital role in influencing an online user's privacy perceptions and behaviours when interacting with online services (Li et al. 2011). Therefore, understanding how an individual's privacy concern influences disclosure of information to a MEAS is important to both MEAS providers and for the success and growth of other location-based services.

This paper brings together research in protective behavior, emergency services management and information systems to better understand what motivates individuals to undertake pre-emptive protective actions such as being willing to use a MEAS. It proposes and tests a model which draws on

Protection Motivation Theory (PMT) which has been used to examine health-related behaviors and in IS to examine security behavior. Key components of the PMT such as an individual's perception of the severity and susceptibility to an emergency, response efficacy and self-efficacy, are combined with privacy concerns to determine their willingness to take pre-emptive actions, in this case, and use a MEAS. This paper reports on an empirical study that investigates individual's willingness to use MEAS, which require the disclosure of personal information. By improving the understanding of users' expectations and concerns, the research expects to provide insights to government agencies and MEAS providers to design and implement better services and perform better risk management.

2 PRIOR RESEARCH

An "emergency" is defined as "a serious, unexpected, and often dangerous situation requiring immediate action." (Oxford Dictionary). It is usually defined in a certain time and space, with a threshold value (e.g. mortality rate) to be recognized. An emergency relates best to response, and usually calls for rules of actions and an exit strategy (WHO, 2016).

Traditional warning systems such as sirens, radio announcements and loudspeakers have proven ineffective and very limited as they are constrained by the emergency personnel and they often do not reach the intended target audience (Sorensen, 2000). Many governments have or are in the process of implementing location-based Mobile Emergency Alert Systems (MEAS) for local and national services. These services provide governments and authorized agencies the ability to provide immediate location-specific communications and information to the public during an emergency. According to the Australian Mobile Telecommunication Association, "The location-based enhancement to Emergency Alert allows emergency warnings to be sent to mobile telephones based on the physical location of the mobile handset at the time of an emergency, including residents and people travelling through a threatened area." (www.amta.org.au). Another Australian organization called Early Warning Network (EWA), provides live severe weather warning across Australia to those who use EWA apps on their mobile devices and allows real-time GPS tracking. In one of the latest warning message issued on 31 March 2017 at 6:12 pm was about potential severe thunderstorms that were going to happen within half-an-hour. Recommended protective actions were provided in the warning message to advise people to "secure loose outside objects", "avoid remaining in the open when storms threaten" and "avoid driving into water or unknown depth and current" (www.ewn.com.au).

Although there are advantages to individuals subscribing to MEAS, prior research shows that location-based services including emergency and risk management services raise issues related to trust, risk perceptions, and privacy concern for users. For example, in an Australian-based study of location-based emergency services, Aloudat and Michael (2011) found that people were in general agreement that there are benefits of such services. However, these benefits rely on the collection of extensive location information and other personally identifying information which raised concerns about privacy such as whether the information collected for emergencies would be used for other purposes without their consent. These findings mirror that of other contexts such as business and social media suggesting that despite the 'public good' aspect of emergency management systems, similar concerns regarding use of personal information may impact individuals' willingness to use such systems and hence, their effectiveness in emergency management (Dinev et al. 2008; Yang et al.,2003; Xu. et al. 2009; 2012). Data privacy risks in particular, have been identified as a factor influencing willingness to use commercial mobile location-based services (Gerpott and Berg 2011).

When it comes to risk assessment, research shows that individuals have different perceptions regarding risks and potential threats (Wildavsky and Dake, 1990), and the meaning they ascribe to a particular threat (such as their perceptions of the severity of and their susceptibility to the threat). This in turn may shed light on the extent of peoples' willingness to use MEAS and disclose their personal information, despite their privacy concerns. Contextual and personal factors may therefore impact people's motivation to take pre-emptive steps to protect themselves from potential harm such that they are willing to give up some of their privacy in return for the benefit of using MEAS that can help mitigate potential harm to people and property.

A number of factors need to be examined to gain a deeper understanding of individual's willingness to use MEAS. These include the nature of an emergency which may arouse individual's fear of a certain threat, the individual's risk perceptions of the threat, how they would like to respond to the potential damage and protect themselves from being hurt by the threat. Prior research suggests that emergencies such as natural disasters present a complex and unpredictable situation with regards to the response actions (e.g. feeling hopeless and doing nothing, or immediately seeking evacuation or taking other protective actions) (Ren et al. 2008). Psychologists (Fritz and Marks, 1954) also point out

that people's emotional reactions to disasters can be very different and these determine their behaviour in disasters. Therefore, understanding individual's risk perception and how to motivate people to take preventive steps becomes important. To address this issue, this study draws on Protection Motivation Theory which aims to explain individual's responses to potential threats (Rogers 1975; 1983), and on privacy concerns, to examine individual's willingness to use MEAS, where such use will involve giving up some privacy in return for the protection that MEAS can enable.

3 RESEARCH MODEL

There are many theories that seek to explain people's protective behaviors including the Health Belief Model (HBM), Theory of Reasoned Action (TRA), and Protection Motivation Theory. Of these, the Protection Motivation Theory (PMT) (Rogers 1975; 1983) is particularly useful due to its inclusion of self-efficacy as a key influence in motivating behavior (Floyd et al. 2000). Central to the PMT is the idea that protection motivation arises from consideration of a potential threat (i.e. 'fear appeals') and one's desire to avoid potential negative outcomes, as embodied in one's attitude and behavioral intention to respond to the potential threat. According to the PMT, coping with a certain threat involves two cognitive appraisal processes in which the behavioral options to mitigate a threat are evaluated (Floyd et al. 2000), that is, a *threat appraisal* and a *coping appraisal*. The threat appraisal identifies the threat and the individuals' perceptions of the severity of and their vulnerability to the threat. This is followed by the coping appraisal which assesses their ability to cope with and avoid the potential threat that is, their response efficacy, self-efficacy and response costs. Together these appraisals are expected to motivate the adaptive response to mitigate the threat (Floyd et al. 2000). In this study, the adaptive (preparedness) response of interest is one's willingness to use a MEAS.

The PMT has been widely used to help explain the influences on and predict various protective behaviors, including protective health-related behaviors such as reducing alcohol use, enhancing healthy lifestyle, and disease prevention (Boer and Seydel, 1996), privacy protection behavior (Youn, 2009), and individual preparedness for disasters such as earthquakes and flooding (Grothmann and Reusswig, 2006; Mulilis and Lippa, 1990). The PMT has also been used alongside privacy concern to predict self-disclosure on social network sites (Kim and Mousavizadeh, 2015).

This study uses Protection Motivation Theory (PMT) to frame the base model for evaluating individual motivation to take preparatory actions in case of an emergency, by using a MEAS. In relation to the threat-response behavior, the model aims to predict people's willingness to use a MEAS, which can potentially reduce their chances of being impacted by or the negative consequences of, an emergency (Floyd et al. 2000). This application of the PMT is extended by incorporating privacy concern to further explain use a MEAS; as this requires the disclosure of personal information this may raise privacy concerns (Aloudat and Michael, 2011). It is expected that while the threat appraisal and coping response may encourage use of a MEAS, privacy concerns may inhibit its use (Aloudat and Michael, 2011; Floyd et al. 2000; Gerpott and Berg 2011; Kim and Mousavizadeh, 2015).

3.1 The Threat Appraisal

According to the PMT, the threat appraisal evaluates one's *perceived vulnerability* to and *perceived severity* of a threat. *Perceived vulnerability* refers to the probability of the threat occurring while *perceived severity* refers to the amount of harm that is associated with the threat (Floyd et al. 2000). Maddux and Rogers (2000) in a study of the ill-effects of smoking found significant effects for perceived severity on intention to adopt a recommended preventive health behavior. Similarly, Vance et al. (2012) in a study of IS Security policy compliance intention found that perceived severity (i.e. the amount of harm that a IS security breach may cause) significantly impacted intention to comply with an organisation's policies. Likewise, Boss et al's (2015) study on the use of anti-virus software, participants who received a high risk message had much stronger intentions to use anti-virus software than those who received a low risk message. Thus, an individual's perceived severity of a threat tends to be positively linked to their intention to perform the protective actions (Ifinedo, 2012).

Prior research on the other hand, has returned mixed findings for the impact of perceived vulnerability on the response action. On the one hand, some studies have shown perceived vulnerability has a significant impact on behavioral intention to take protective actions (Ifinedo, 2012; Lee and Larsen, 2009). In Wurtele's study (1988), a group of female students who received information about osteoporosis showed a strong belief in their vulnerability to osteoporosis, which in turn, had a positive impact on their intention to increase calcium-rich food. However, others have found that perceived vulnerability is not a consistent predictor (Johnston and Warkentin, 2010). For example, Vance et al. (2012) found that perceived vulnerability (i.e. employees' assessment of the organization's

vulnerability to IS security threats if they took no steps to prevent them) was not significant in relation to IS security policy compliance intention. Boss et al. (2015) on the other hand found that in a high fear-appeal setting perceived vulnerability was significant, but in a low fear-appeal setting, vulnerability was not significant. Boss et al. (2015) concluded that when the fear-appeal is strong (for example, a high risk message is received) the core PMT is supported, but when fear-appeal is weak, the PMT may not hold. This finding is consistent with prior work that suggests when it comes to risk assessment, that individuals have different perceptions regarding risks and potential threats (Wildavsky and Dake, 1990), and the meaning they ascribe to a particular threat (e.g. perceived severity and susceptibility to the threat). In this study, consistent with the PMT, we assess both components of the threat appraisal. As such we expect:

H1: Perceived severity of an emergency is positively related to willingness to use a MEAS.
H2: Perceived vulnerability to an emergency is positively related to willingness to use a MEAS.

3.2 The Coping Appraisal

Appraisal of a threat can result in an adaptive response when an individual believes they are able to cope with the threat and avoid possible danger (Floyd et al. 2000). Key components of the coping appraisal are efficacy (i.e. response efficacy and self-efficacy) and response costs. *Self-efficacy* refers to an individual's belief that they can do what is required to minimize a threat, while response efficacy concerns the degree to which a person believes that their protective action will be effective in protecting themselves (Floyd et al. 2000; Maddux and Rogers, 1983). Response costs on the other hand, refer to any costs (e.g. monetary, time, effort) that are associated with the adaptive response (Floyd et al. 2000). While response efficacy and self-efficacy will increase the likelihood of the response action, response costs will decrease it (Boss et al. 2015; Floyd et al. 2000). For a positive coping-response to occur, when faced by a threat, persons must believe they are both capable of taking action and that such action would be effective in mitigating the threat, and that the cost of taking action is less than the benefits (Boss et al. 2000). Given the need to disclose personal information and concerns that persons may have, it is further expected that the coping-response appraisal, will also consider the extent of their privacy concerns alongside the coping appraisal, such that increased privacy concerns will elevate the perceived cost of the adaptive response, and lower its likelihood.

Prior research suggests response efficacy is one of the best predictors of protective behavior intention regardless of the research context (Boss et al. 2015; Ifinedo, 2012; Lee, 2011; Wurtele, 1988). In Wurtele's study (1988) of female students' perceptions about osteoporosis, response efficacy was the second-best predictor of intention to increase calcium-rich food in the diet. In a study on anti-plagiarism software adoption (Lee, 2011), response efficacy was the only construct in the coping appraisal that had a direct significant impact on adoption. Boss et al. (2015) in their study of malware software use and nonuse found that response efficacy was a consistent predictor of intention regardless of whether the pop-up warning regarding malware signaled a high or low-risk situation.

In this study, *self-efficacy* refers to an individual's belief in their ability to use a MEAS (Floyd et al. 2000). The inclusion of self-efficacy as a distinct factor in the PMT is a key element that distinguishes the PMT from other theories such as the Health Belief Model (Floyd et al. 2000). In studies using the PMT, self-efficacy has been shown to be a promising predictor of behavioral intention (Boer and Seydel, 1996; Ifinedo, 2012; Maddux and Rogers, 1983). In a study by Ifinedo (2012), persons with higher self-efficacy were more willing to comply with information system security policy (ISSP) than those who had lower level of self-efficacy. Consistent with the PMT, since using a MEAS can be expected to help persons to mitigate a threat by taking the recommended actions, it is expected that:

H3: Response efficacy is positively related to willingness to use a MEAS.
H4: Self-efficacy is positively related to willingness to use a MEAS.

A coping appraisal weighs response efficacy and self-efficacy against perceived costs, where the cost of carrying out an adaptive behaviour limits protection motivation (Boer and Seydel, 1996). For example Boss et al. found response cost to be a consistent predictor of intention across a high and low fear appeal situations. For MEAS users, *response costs* may include monetary costs such as payment for data usage and to receive alert messages, as well as non-monetary costs such as the time and effort needed to add and maintain personal information in a MEAS such as health status. Likewise, it is expected that the cost of using a MEAS may reduce willingness to use a MEAS. Hence:

H5: Response cost is inversely related to willingness to use a MEAS.

Prior research suggests that the collection of a significant amount of personal data for personalizing services may impact an individual's privacy concern (Beresford and Stajano, 2013). Given that in the

context of MEAS use, location data from mobile devices are continuously collected, this is likely to raise concerns about privacy. Even where personal information is not continuously collected, privacy concerns may also act as an inhibitor to one's use of systems that require its disclosure (Dinev et al., 2008; Yang et al.,2003; Xu., et al., 2009; 2012). For example, Aloudat and Michael (2011) found that people were concerned about whether information collected for emergencies would be used for other purposes without their consent. Gerpott and Berg (2011) in a study of commercial mobile location-based services found that data privacy risks inhibited willingness to use these services. Given prior findings of a negative relationship between privacy concern and willingness to disclose personal information to use services that collect personal information, it is expected that individuals with heightened privacy concern in relation to MEAS will be less willing to use it. Hence, it is expected:

H6: Privacy concern is inversely related to willingness to use a MEAS

Figure 1 summarises the research model.

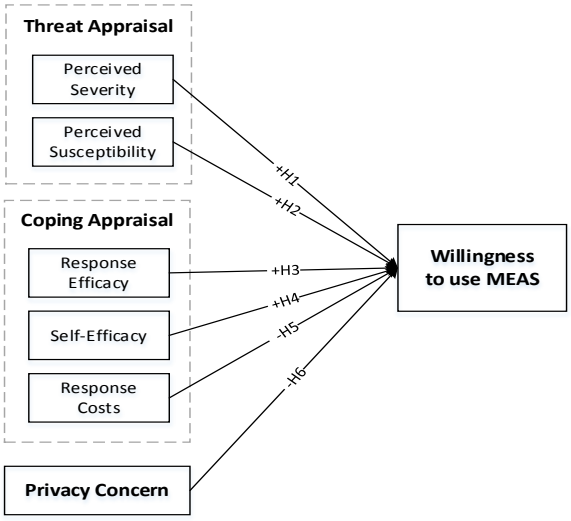

Figure 1: The Research Model

4 METHODOLOGY

Participants for this study were recruited from across New Zealand, and asked to complete an online survey. The study uses a hypothetical scenario to present respondents with a potential flood situation and recommended actions. With floods being the most frequent and costly of natural disasters in New Zealand, the choice of situation is both realistic and familiar to respondents. The target audience are mobile device users, 18 years and over. This paper reports the findings from 103 respondents recruited from the South Island and Wellington regions of New Zealand. Of these, 60 (58.3%) were female and 42 (40.8%) were male (1 response missing); 36 persons (35%) were aged 35 years and under; 31 (30%) were aged 35-50 years and the remainder (n=36, 35%) were over 5o years. 80.6% (n=83) of the respondents resided in urban areas and 18.4% (n=19) in rural areas (1 response missing).

All constructs for this study (Appendix A) were assessed using existing scales adapted to the context of using MEAS. Perceived susceptibility (4 items), perceived severity (5 items), response efficacy (3 items) and behavioral intention (3 items) were adapted from Milne et al (2000) and Johnston and Warkentin (201o). Self-efficacy (3 items) and response cost (6 items) were likewise adapted from prior studies (Ifinedo, 2012; Meso et al. 2013; Myyry et al. 2009; Woon et al. 2005).

5 DATA ANALYSIS and RESULTS

To examine the research model, this study uses partial least squares path modeling (PLS-PM). The PLS-PM approach is a component-based approach to structural equation modeling that has been widely used to evaluate use of new technologies including location-based mobile technologies and services (e.g. James et al. 2015; Xu et al. 2012). The approach allows for the simultaneous evaluation of the measurement model and the structural model. It is also suitable when formative measures are included (e.g. response cost) and the goal of the research is to predict the 'target' construct and identify key 'driver' variables (Hair, et al. 2014). SmartPLS 3.2.3 was used to assess the research model and bootstrapping (using 500 resamples) used to evaluate the significance of the model paths.

For the measurement model the focus for assessing reflective constructs is on internal consistency, reliability, and convergent and discriminant validity. The results showed the item loadings ranged from 0.702 to 0.969 exceeding the recommended threshold of 0.708 for indicator reliability (Hair et al. 2017). Composite reliabilities ranged from 0.922 to 0.957 and average variance extracted (AVE) from 0.713 to 0.882 also exceeding suggested cut-offs of 0.70 and 0.50 respectively (Hair et al. 2017). Using the Fornell-Larcker criterion to assess discriminant validity, the results showed the square root of the AVEs for all constructs were greater than the correlations associated with other constructs, satisfying this test.

Response cost (Woon et al. 2005) captured monetary and non-monetary costs and was modeled as a formative construct; two criteria were examined - collinearity (VIF values), and indicator weights and loadings. The results showed VIF of less than 5, suggesting that collinearity was not an issue (Hair et al. 2017). Indicator weights, signaling the relative importance of each item, ranged from -0.208 to 0.722 with COST3 being the only indicator with a significant weight (0.722, $p \leq 0.01$). Absolute importance of the indicators (i.e. loadings) was also examined; these ranged from 0.249 to 0.966, with COST1 (0.272) and COST4 (0.249) falling below 0.50, so of little importance in the current context. Since these items were theoretically relevant to and in line with recommended approaches to measuring cost, they were retained in the research model (Hair et al. 2017; Woon et al. 2005). However, it is suggested that these measures be revisited in future work.

Next, the structural model was examined. The model accounted for 0.597 of the variance observed for intention to use MEAS. For threat appraisal, perceived severity (-0.168, $p \leq 0.020$) and perceived susceptibility (-0.148, $p \leq 0.019$) were significant with respect to intention. All three hypotheses (H3-H5) concerning the coping appraisal and intention were also supported, that is, response efficacy (0.350, $p \leq 0.001$), self-efficacy (0.273, $p \leq 0.002$), and response costs (-0.171, $p \leq 0.03$). As expected, privacy concern (-0.188, $p \leq 0.010$) was inversely related to intention, supporting H6.

5.1 Limitations

Notwithstanding the contributions to knowledge, there are some limitations to address in future work. First, the study focused on mobile users in New Zealand; it also used a vignette (emergency scenario) that is familiar to the audience, but may not be as relevant to others. To extend generalizability, future studies could test the model with other contexts such as bushfires in Australia and tornados in the USA. Second, the technology itself (MEAS) is not widely available, and where it is available, there is little uptake. Thus most respondents were evaluating a technology they had little or no direct experience with. At the same time, it is useful to note that more MEAS are currently under development in New Zealand, particularly following the severe damage caused by the magnitude 7.8 Kaikoura earthquake, in November 2016 (Stuff, 2017). So although responses in this hypothetical context may not match exactly near-term behaviors, the findings can provide insights that may usefully inform MEAS development and implementation. Future research can also collect data for both intention and actual behavior when the newly developed MEAS are available. Similar studies can also be conducted in countries such as Australia and Japan that have well-established MEAS. Finally, research suggests other factors such as fear and trust (Aloudat and Michael, 2011; Floyd et al. 2000) may also impact willingness to use MEAS; these may be assessed in future work.

6 CONCLUSION

Using Protection Motivation Theory as a theoretical lens, this study examines the tradeoff between privacy concern and, two key elements in individual protection behavior, that is a threat appraisal and coping appraisal, to better understand individual's willingness to use location-based mobile emergency alert service, as a pre-emptive step in emergency preparedness.

Using survey data collected from mobile users in New Zealand and a description of a potential threat (i.e. flooding), empirical evidence suggests that coping appraisal acts as the stronger predictor of willingness to use MEAS. Of the components, response efficacy was the most impactful followed by self-efficacy, while response costs and privacy concern inhibited use of MEAS. The threat appraisal (both perceived severity and vulnerability) was also significant in motivating willingness to use MEAS.

Taken altogether, the findings contribute valuable insights to the literature. In relation to the PMT, the study extends the application of the PMT alongside privacy concern in to the emergency management literature. While response efficacy and self-efficacy both serve as enablers of the coping appraisal, response cost (in particular the effort needed to update and maintain personal information in a MEAS) alongside privacy concern inhibited preparedness intention, in relation to MEAS use. In other words, while individuals may perceive themselves able to use a MEAS and its use as effective in protecting

themselves, concerns about privacy and response costs may inhibit uptake. This suggests that for MEAS to be successful service providers need to allay individuals' concerns about how data collected for use in emergency situations is handled (Aloudat and Michael, 2011) and minimize the cost and effort needed to use these systems. It also provides insights that can be used by service providers and government agencies as they seek to design and implement better MEAS for future use.

7 References

Aloudat, A. and Michael, K. (2011). Toward the regulation of ubiquitous mobile government: a case study on location-based emergency services in Australia. *Electronic Commerce Research*, 11(1), 31-74.

Beresford, A. R. and Stajano, F. (2003). Location privacy in pervasive computing. *IEEE Pervasive* computing, (1), 46-55.

Boer, H. and Seydel, E. R. (1996). *Protection motivation theory*. 95-120.

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

Dinev, T. Hart, P. and Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance – An empirical investigation. *Journal of Strategic Information Systems*, 17(3), 214-233.

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

Gerpott, T. and Berg, S. (2011) Determinants of the willingness to use mobile location-based services, *Business and Information Systems Engineering*, vol 5, 279-287.

Grothmann, T., & Reusswig, F. (2006). People at risk of flooding: why some residents take precautionary action while others do not. *Natural Hazards*, 38(1), 101-120.

Hair, J. F. Hult G. M. Ringle, C. M. (2017). A primer on partial least squares structural equation modeling (PLS-SEM). Thousand Oaks, Calif: SAGE Publications.

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

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.

James, T. L. Warkentin, M. and Collignon, S. E. (2015). A dual privacy decision model for online social networks. *Information and Management*, 52(8), 893-908.

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

Kim, D. and Mousavizadeh, M. (2015). A Study of the Effect of Privacy Assurance Mechanisms on Self--disclosure in Social Networking Sites from the View of Protection Motivation Theory. *Proceedings: Americas Conference on Information Systems*, Puerto Rico 10pp

Kim, E. and Lee, B. (2009). E--service quality competition through personalization under consumer privacy concerns. *Electronic Commerce Research and Applications*, 8(4), 182-190.

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

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.

Maddux, J. E. and 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, N. K. Kim, S. S. and Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, 15(4), 336-355.

Milne, S. Sheeran, P. and Orbell, S. (2000). Prediction and intervention in health---related behavior: A meta--analytic review of protection motivation theory. *Journal of Applied Social Psychology*, 30(1), 106-143.

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.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 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.

Sorensen, J. (2000), Hazard warning systems: Review of 20 years of progress, *Natural Hazards Review*, 1(2), 119-125.

Wildavsky, A. and Dake, K. (1990). Theories of risk perception: Who fears what and why? *Daedalus*, 41-60.

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

Wurtele, S. K. (1988). Increasing Women's Calcium Intake: The Role of Health Beliefs, Intentions, and Health Value. *Journal of Applied Social Psychology*, 18(8), 627-639.

Xu, H. Teo, H. H. Tan, B. C. Y. and Agarwal, R. (2009). The Role of Push--Pull Technology in Privacy Calculus: The Case of Location--Based Services. *Journal of Management Information Systems*, *26*(3), 135-174.

Xu, H. Teo, H.-H. Tan, B. C. Y. and Agarwal, R. (2012). Research Note- Effects of Individual Self--Protection, Industry Self--Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services. *Information Systems Research*, *23*(4), 1342-1363

Yang, Z. Peterson, R. T. and Cai, S. (2003). Services quality dimensions of Internet retailing: an exploratory analysis. *Journal of Services Marketing*, 17(7), 685–700.

Appendix A: Sample Items

Perceived severity	If I were affected by an emergency situation like this ... it would be serious.
Perceived vulnerability	My chances of being affected by an emergency situation like this in the future are high.
Self-efficacy	I feel confident in my ability to use a personalised MEAS.
Response efficacy	Using a personalised MEAS would be a good way to reduce my risk of being affected by an emergency situation.
Response cost	It would be time-consuming to maintain my personal profile in a personalised MEAS (e.g. updating my mobile number, address, health status, etc.).
Privacy concern	It would bother me if a personalised MEAS provider were to ask me for personal information.
Willingness to use MEAS	If personalised Mobile Emergency Alert Service (MEAS) were available to you ... I intend to use a personalised MEAS.