AIS Transactions on Human-Computer Interaction

Volume 3 | Issue 3 Article 2

Fall 9-26-2011

Social Networking Websites and Posting Personal Information: An Evaluation of Protection Motivation Theory

Kent Marett
Mississippi State University, kmarett@cobilan.msstate.edu

Anna L. McNab
Niagara University, amcnab@niagara.edu

Ranida B. Harris
Indiana University, rbharris@ius.edu

Recommended Citation

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. Retrieved from https://aisel.aisnet.org/thci/vol3/iss3/2
DOI:

AIS Transactions on Human-Computer Interaction

Transactions on Human-Computer Interaction

THCI

Original Research

Social Networking Websites and Posting Personal Information: An Evaluation of Protection Motivation Theory

Kent Marett
Mississippi State University
kmarett@cobilan.msstate.edu

Anna L. McNab
Niagara University
amcnab@niagara.edu

Ranida B. Harris
Indiana University
rbharris@ius.edu

Abstract

The popularity of social networking websites among Internet users continues to grow, even though social networking remains a risk for users who do not participate with caution. Using protection motivation theory (PMT) as a theoretical lens to provide a research model, and by issuing a fear appeal to social network users about the potential threat to their privacy, this study identified perceptions and beliefs held by users that influence their behavioral responses to the imposed threats. A snowball sample survey measuring the variables conceptualized by PMT was completed by 522 social network users. A time-ordered hierarchical regression analysis of the responses showed that PMT provides explanations for both adaptive and maladaptive responses, particularly for the response of hopelessness. Implications and directions for future research in this area are offered.

Keywords: Social networking, online privacy, protection motivation, risk assessment, user behavior, adaptive response, maladaptive response

Ping Zhang was the accepting Senior Editor. This article was submitted on 3/26/2010 and accepted on 7/5/2011. It was with the authors 254 days for 2 revisions.

Marett, K., A. L. McNab, and R. B. Harris (2011) "Social Networking Websites and Posting Personal Information: An Evaluation of Protection Motivation Theory," *AIS Transactions on Human-Computer Interaction* (3) 3, pp. 170-188.

INTRODUCTION

The Internet has introduced a myriad of networked applications that have been heartily adopted by the general public, perhaps none more so than websites that facilitate social networking. A recent survey estimates that there are a combined 2.3 billion registered users for the ten most popular social networking websites worldwide (Socialnomics, 2011). An analysis of Internet traffic during the spring of 2011indicated that 2.1 percent of the bandwidth utilized in North America is devoted to social networking (Sandvine, 2011). It is reasonable to expect that social networking will remain popular around the world for the foreseeable future.

Social networking websites allow users to "convey their self or multiple selves" online by displaying personal information and pictures for others to see (Schau and Gilly, 2003). The users of these services commonly state that the websites provide an easy and entertaining way for them to keep in contact with remote friends and family, as well as for meeting new people with common interests, both platonically and romantically (Gibbs et al., 2006; Valkenburg et al., 2006). Unfortunately, these communities are also prime targets for online predators and troublemakers. Arrests have been made around the country for instances of cyberbullying, cyberstalking, identity theft, and sexual harassment. Legislators in both the U.S. House of Representatives and the Senate have recently introduced bills that seek to protect social network users by requiring sex offenders to register their online identities, as well as prohibiting people from misrepresenting their ages and other information when attempting to engage in sexual activity with minors. Despite the efforts of lawmakers, social network users are not completely safe unless they practice discretion in regards to with whom they communicate and what information they post about themselves on their personal profiles.

At the most fundamental level, social networking websites can be defined as "a category of community sites that have profiles, friends, and comments" (Boyd, 2007). Profiles refer to the personal pages that individual users can register for, develop, and update with content and graphics for other visitors to view. Friends are the visitors to a user's profile who formalize a relationship with the user by reciprocally subscribing to the user's profile. Comments are the text-based (sometimes supplemented with graphics or videos) messages friends post to others' profiles (Boyd, 2007). Social network users often develop profiles that present themselves publicly in ways that meet personal goals, and this can involve the use of their own personal information. While many users make their personal information available to others for the enjoyment of social acknowledgments (e.g., posting one's birth date in order to receive well-wishes from friends), it is not uncommon for some users to engage in impression management (Boyd and Ellison, 2007), even to the point of exposing more information than they normally would in another environment.

Unfortunately, social networking websites also seem to be well suited for those with ill will. Predators seem to be emboldened through a process of online disinhibition, primarily because of what Barak and Fisher (2002) call the "Penta-A Engine," composed of the Internet attributes of anonymity, availability, affordability, acceptability, and aloneness. Their targets' demographics are wide-ranging, but a recent report indicates that a majority of past crimes initiated over the Internet victimized adolescents between the ages of 13 and 17, and 75 percent of the reported victims were female (Wolak et al., 2004). Traditionally, victimization has been associated with risky behavior performed by the victims themselves, such as chatting with strangers online or submitting personal information in chat rooms (Mitchell et al., 2001). In 2010, Harris Interactive conducted a McAfee study4 with 955 teenagers between 13 and 17 years of age, and found that 69% of teenagers included their physical location in a social networking status update and 24% have shared their e-mail address and chatted with strangers. However, exploitable information does not have to be submitted in real-time to produce vulnerability as users' profiles create information archives for all interested parties; this information can be misused even at a later time. In a discussion of exploitable information, Criddle (2006) advised social networkers to refrain from making their entire name, friends' and family members' names, home addresses, phone numbers, and the locations of where one might go to school or work public without serious consideration of the risks. An experiment conducted by Sophos Labs claimed that 46% of Facebook users willingly make personal information public on their profiles, including phone numbers, email addresses, and their date of birth, making them susceptible to identity theft or worse[1]. In fact, Criddle suggested that savvy social engineers may be able to use other personal information, for example, that a user might be "lonely or fighting with parents," or that a user's house "will be empty next week" (p.72), in an effort to either ingratiate themselves to the user or to elicit even more information from the user's friends.

Despite news stories, warnings, and even legislation, most social network users do not seem to alter their risky behavior of disclosing personal information online (Rosenblum, 2007). For users, the act of establishing a profile is motivated by the desire to publicize oneself. The rewards derived from posting personal information and socializing with friends doing likewise seemingly outweigh the potential danger for social network users at risk. With motives of keeping contact with old friends and meeting new friends, limiting one's self-disclosure online may not be an attractive option regardless of the possible dangers (Tufekci, 2008). Also, many users are simply uninformed about online threats to their privacy and actions they can take to protect themselves (Paine et al., 2007). Additionally, the security controls of social networking websites are often intentionally weaker than they should be in order to make

registration and information sharing easy for users (Acquisti and Gross, 2006). The most secure option for social network users is not to post personal information in the first place. This leads to the following research question:

> *What factors influence an individual to post personal information, and further, what factors influence the individual to discontinue posting personal information after being informed about the potential risk to one's privacy and safety?*

The purpose of this study is to investigate how computer users respond to information about online threats when considering what personal information they choose to release. The outline of the paper is as follows. First, we review the relevant literature on protection motivation and integrate it with literature on online threat assessments. Using this prior research we derive hypotheses that deal with the responses to threat information for social networking users. Next, we detail the survey method used to test our hypotheses. Following a report of the results, we discuss our findings and the implications they have for future research and for social networking users themselves.

In order to examine the influence that information about potential online threats has on the recipients' intention to adapt online information sharing behavior, we draw from protection motivation theory (PMT), a theoretical framework used in the field of health communication. Originally developed by Rogers (1975), PMT focuses on the ways in which individuals respond to receiving threatening information about activities and pastimes that they may be currently engaged in. PMT was developed to help identify the influences that can sway a person's response to the information and ultimately lead them to the appropriate response, ensuring their safety or well-being. Over time, PMT has been used to explain the choices made by an individual when deciding whether to continue to engage in the activity or to better protect oneself (Maddux, 1993). The threatening activities previously studied were primarily health-related, involving topics such as sun tanning and skin cancer (McMath and Prentice-Dunn, 2005), lack of exercise (Fruin et al., 1991), sexually transmitted diseases (Tanner et al., 1991), and smoking (Maddux and Rogers, 1983), but research using PMT has also addressed reactions to other threats, including earthquake preparedness (Mulilis and Lippa, 1990), flood preparedness (Grothmann and Reusswig, 2006), and traffic safety (Sonmez and Graefe, 1998). This line of research revealed that while many people decided to heed the information about threats, others simply chose to ignore the same information and continue with the risky behavior.

Over the years, PMT has been found to provide explanations for individuals' behavioral intentions over a robust range of situations. However, PMT has seldom been applied to individuals' risky use of the Internet and information technology, with exceptions including recent studies on computer users' decisions to employ virus protection (Lee et al., 2008) and to regularly back up work-related data (Boss and Galletta, 2008), employees' compliance with company security policies (Pahnila et al., 2007; Johnston and Warkentin, 2010), and the stress coping mechanisms for IT professionals (Tsai et al., 2007). Other recent studies have utilized some of the same health-related constructs modeled in PMT to help explain security consciousness in users (Ng et al., 2009). The results of these studies largely indicated that the same factors that influence an individual's response to health and environmental threats, such as response costs, efficacy, and vulnerability, can influence an individual's response to technology-related threats. Despite the fact that these studies focused primarily on behavioral intentions to adapt one's behavior in the face of security threats (Liang and Xue, 2009; Siponen et al., 2010), no studies have yet linked PMT to the risks associated with making one's personal information publicly available online. We believe that PMT has the potential to help explain the risk assessment and subsequent behavioral changes performed by social networking users.

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 behavior (Rogers and Prentice-Dunn, 1997). The fear appeal involves an information intervention targeting the risky behavior in an attempt to influence an individual's safety (Milne et al., 2000). PMT seeks to explain the cognitive mechanisms the individual undertakes upon receiving information about the threat, which manifest themselves in two distinct but related processes, a "threat appraisal" and a "coping appraisal" (a schematic model of the processes is displayed in Figure 1 below). While the original PMT model conveys a parallel process model, meaning both the threat and coping appraisal processes occur at the same time (Rogers, 1975), others have argued that the processes occur in sequential order, with the threat appraisal occurring before the coping appraisal (Norman et al., 2005; Tanner et al., 1991). Lazarus (1991) describes the primary appraisal as focusing on the threat at hand, with the secondary appraisal focusing on ways to cope with the threat. Tanner and colleagues (1991) state that this order of processes occurs out of necessity, as individuals cannot be expected to appraise coping options without first considering the nature of the threat and how it personally affects them. We discuss the two processes and their related variables found in the PMT model below.

Upon receiving threatening information, an individual initially engages in a process of "threat appraisal," which involves assessment of the risk to their personal safety (McClendon and Prentice-Dunn, 2001). Perceived risk includes an evaluation of how susceptible the person believes he or she is to the threat, as well as how serious the consequences would be should the threat be realized (Milne et al., 2000). During the threat appraisal process, perceptions of the threat are weighed against the intrinsic and extrinsic rewards the person receives from the risky behavior. Intrinsic rewards include the physical and psychological pleasure that is derived from the behavior, while extrinsic rewards are the increases of status, reputation, and general approval from one's peers as a result of

engaging in the behavior (McClendon and Prentice-Dunn, 2001). During the threat appraisal process, if the rewards outweigh the perceived risks, the individual is likely to proceed with a "maladaptive response" which fails to protect the person and continues to leave him or her vulnerable (Floyd et al., 2000). Maladaptive responses can ultimately lead to ego-defense behaviors like avoidance and hopelessness and serve to reduce the level of fear instead of reducing the threat (Rippetoe and Rogers, 1987). According to Witte (1992), avoidance involves a defensive resistance to information advising an individual on how to reduce the risk associated with the threat of interest. Avoidance behaviors can include active inattention to the message or active suppression of thoughts about the threat. Hopelessness refers to the individual's belief that the threat is unavoidable no matter what he or she does, a response that often results in a person continuing the risky behavior (Rippetoe and Rogers, 1987).

Finally, perceptions of "fear" are related to the anxiety an individual feels because of perceived vulnerability to the threat, as well as the perceived severity of the consequences presented by the threat (Milne et al., 2000). Fear is considered to be an emotional outcome that may be aroused when an individual considers the likelihood of the threat at hand, and can serve as a catalyst heightening the threat and coping appraisal processes (Norman et al., 2005). The effect of fear is related to perceptions of the threat itself, with the perceptions of the risk involved having an influence on the degree and intensity of the individual's response (Lazarus, 1991). For some people, maladaptive responses are chosen as a way for the person to deal with fear, as opposed to being a rational method for protection from the threat itself (Rippetoe and Rogers, 1987; Witte, 1992). On the other hand, fear has also been observed as increasing a person's motivation to respond in an adaptive, protective manner (Tanner et al., 1991). For the purposes of this study, we view fear as an intervening variable which provides the impetus for a threatened individual to precede with the appraisal processes.

The second cognitive mechanism, which takes place following the threat appraisal (Grothmann and Reusswig, 2006), is the "coping appraisal." In this process, the person appraises his or her ability to reduce the risk of the threat. During a coping appraisal, the two major factors the individual evaluates are response efficacy, which is the belief that a proposed countermeasure will be effective in averting the threat, and self-efficacy, which is the belief that one can successfully implement the countermeasure (McClendon and Prentice-Dunn, 2001). In the coping appraisal process, these two efficacy variables are compared to response costs, which are the monetary, time, and effort costs required to carry out the defense. Higher response and self-efficacies lead to a better chance the person will choose an adaptive behavioral response, while higher response costs decrease the probability of an adaptive response (Floyd et al., 2000). Adaptive responses include intentional changes to one's behavior made in order to reduce or eliminate the risk associated with the threat (Fry and Prentice-Dunn, 2005). When a person makes the conscious decision to make an adaptive response to the threat, he or she can be said to be engaged in protection motivation (Grothmann and Reusswig, 2006), as illustrated in Figure 1.

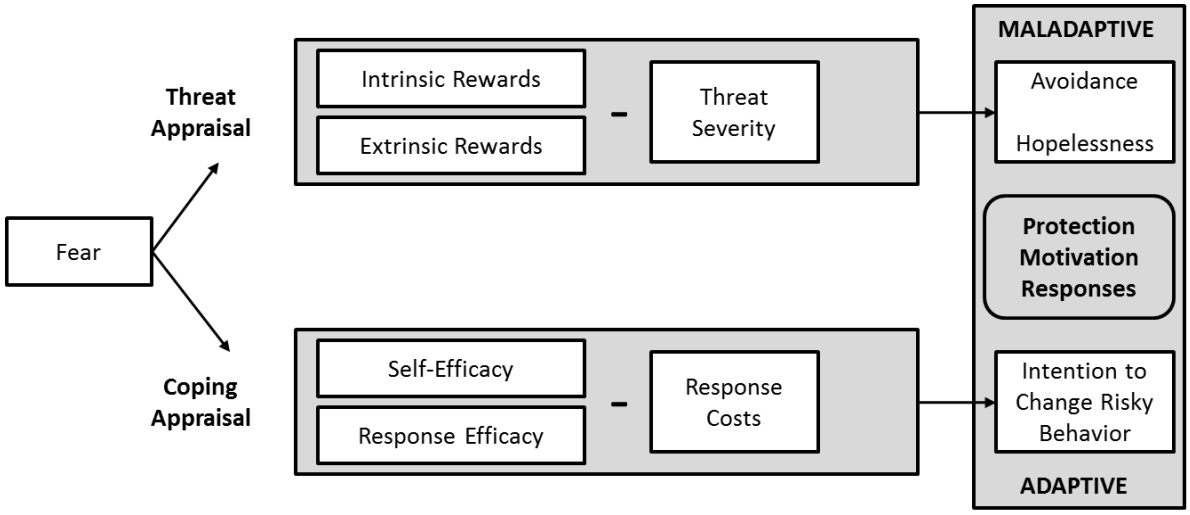

Figure 1: A Schematic Model of the Cognitive Processes Described by Protection Motivation Theory. Adapted from Floyd et al. (2000)

According to PMT, the outputs of the threat appraisal and coping appraisal processes should predict the effects of the fear appeal information, and these effects are usually measured in PMT research as behavioral intentions (Rogers and Prentice-Dunn, 1997). An example of the manner in which PMT demonstrates how the conflicting influences of the model variables affect a person's behavioral intentions to either resume or curtail the risky behavior is the skin cancer intervention conducted by McClendon and Prentice-Dunn (2001). Participants in the study read material emphasizing the increased risk of skin cancer posed by sunbathing, especially without the application of sunscreen.

Because individuals who engage in excessive sun tanning often do so for intrinsic enjoyment as well as the extrinsic reward of improving one's appearance (Leary and Jones, 1993), the fear appeal also described the eventual deleterious effects of sunbathing on one's skin. Immediately following the fear appeal, subjects reported higher risk perceptions and higher efficacy for reducing the risk, as well as a reduced influence of the rewards from sunbathing and lower perceived response costs associated with ending the risky activity. Over 70 percent of the subjects receiving the intervention reported intentions to quit sunbathing, and the longitudinal effectiveness of the fear appeal was demonstrated when those subjects were observed with lighter skin a month later. In comparison, subjects in a control group who did not receive any fear appeal information continued to maintain their previous perceptions and beliefs about sunbathing. For instance, the control group reported significantly higher intrinsic and extrinsic motivations for sunbathing and significantly lower risk perceptions, resulting in significantly lower intentions to quit sunbathing. For the control group, concern over personal appearance often overrode any pre-existing knowledge on the dangers of sunbathing (McMath and Prentice-Dunn, 2005).

The purpose of the present study is to extend the prior research on protection motivation into the arena of online social networking and information privacy. Privacy experts recommend to social network users that they cease posting their personal information on their profiles, a suggestion that serves as the adaptive response in this study. 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 he or she has the ability and the confidence to make necessary changes (self-efficacy) (Rogers and Prentice-Dunn, 1997). Therefore, according to PMT, social network users who perceive the potential risk of posting personal information as being high, or who believe in their ability to follow the recommended privacy changes and remove personal information, or who believe the recommended changes are capable of preventing personal information from being exploited are more likely to make the adaptive response. Likewise, other PMT variables, like intrinsic and extrinsic rewards and response costs will reduce the chance for an adaptive response. In other words, if a social network user highly enjoys the gratification one receives from posing personal information, if he or she believes posting personal information will influence his or her status or reputation within the network, or if the costs associated with removing personal information throughout his or her profile are undesirably high, we expect the likelihood that the social network user will remove and cease posting personal information will be reduced. We expect that these PMT variables can help explain a social network user's decision to not post their personal information.

- H1A: Perceived threat severity will be positively associated with the adaptive response to remove one's personal information from a social networking profile.
- H1B: Self-efficacy will be positively associated with the adaptive response to remove one's personal information from a social networking profile.
- H1C: Response efficacy will be positively associated with the adaptive response to remove one's personal information from a social networking profile.
- H1D: Intrinsic rewards will be negatively associated with the adaptive response to remove one's personal information from a social networking profile.
- H1E: Extrinsic rewards will be negatively associated with the adaptive response to remove one's personal information from a social networking profile.
- H1F: Response costs will be negatively associated with the adaptive response to remove one's personal information from a social networking profile.

Based on the past literature, PMT variables can also be expected to increase the likelihood of a maladaptive response. These variables include the importance of the intrinsic and extrinsic rewards derived from conducting the risky behavior, as well as how costly changing the risky behavior is perceived to be by the individual (Rogers and Prentice-Dunn, 1997). The maladaptive responses investigated in this study are avoidance and hopelessness. With either avoidance or hopelessness, as described earlier, the risky behavior continues, and the social network user's personal information is still vulnerable.

Much prior research using PMT has not accounted for the likelihood of an individual opting for a maladaptive response, instead focusing solely on the adaptive response captured as the intentions to change the risky behavior (Norman et al., 2005). However, a few prior studies have examined the influence of PMT variables on maladaptive responses, and the results tend to support the processes described in the schematic PMT model. For example, intrinsic and extrinsic rewards can be expected to increase the chances a maladaptive response will be selected, as individuals who rate their desire for those rewards as high are likely to forsake their own safety or health (Floyd et al., 2000, Rippetoe and Rogers, 1987). Also, high perceptions of response costs associated with changing the behavior have been found to predict maladaptive responses (Abraham et al., 1994). There is also evidence of negative relationships with maladaptive responses for both self-efficacy and response efficacy variables (Ben-Ahron et al.,

1995, Orbell and Sheeran, 1998), meaning that individuals who doubt their own ability to protect themselves or believe the suggested changes from experts are inadequate for their protection are more likely to engage in a maladaptive response. Likewise, prior work provides evidence that individuals who believe they are vulnerable to a severe threat will choose a maladaptive response out of anxiety (Seydel et al., 1990). These results, which originate from a wide field of different domains, give rise to the following set of hypotheses (all of which are summarized in Figure 2 below):

- H2A: Intrinsic rewards will be positively associated with the maladaptive response to continue posting one's personal information to a social networking profile through avoidance or hopelessness.
- H2B: Extrinsic rewards will be positively associated with the maladaptive response to continue posting one's personal information to a social networking profile through avoidance or hopelessness.
- H2C: Response costs will be positively associated with the maladaptive response to continue posting one's personal information to a social networking profile through avoidance or hopelessness.
- H2D: Perceived threat severity will be negatively associated with the maladaptive response to continue posting one's personal information to a social networking profile through avoidance or hopelessness.
- H2E: Self-efficacy will be negatively associated with the maladaptive response to continue posting one's personal information to a social networking profile through avoidance or hopelessness.
- H2F: Response efficacy will be negatively associated with the maladaptive response to continue posting one's personal information to a social networking profile through avoidance or hopelessness.

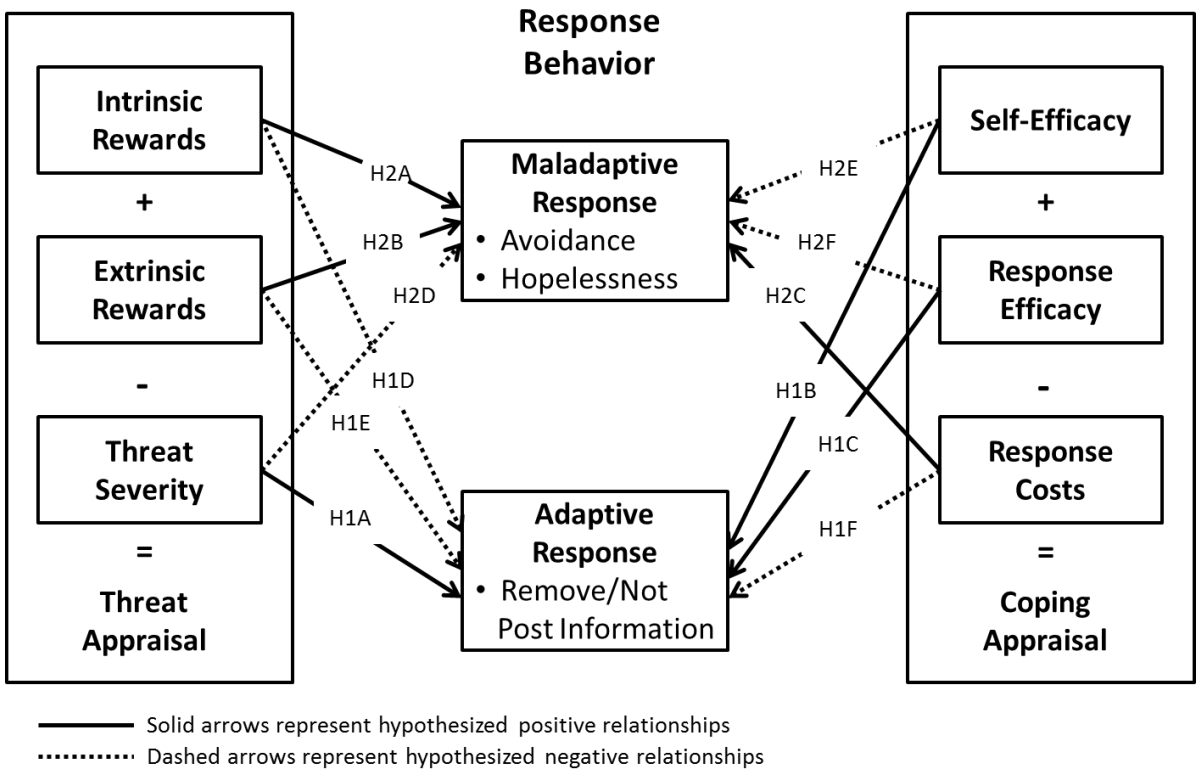

Figure 2: Research Model

The existing literature on PMT has given little attention to individual and demographic differences like gender, even though some researchers have called for assessments of PMT along those lines (McClendon and Prentice-Dunn, 2001). However, there is existing research on risk assessment between genders that can provide guidance toward predicting and explaining how males and females might respond to information about social networking threats. It should first be stated that women are frequently considered to be more risk averse across many different situational contexts than men, although in some contexts, the differences between the genders are more trivial than others (Gustafson, 1998, Jianakoplos and Bernasek, 1998). A meta-analysis of 150 studies of risk suggests that men and boys take more risks, even when it is clear they should not, whereas women and girls often do not take risks even in

situations when they would benefit from doing so (Byrnes et al., 1999). Gender research in IS also indicates that males and females can be expected to respond to information regarding system use differently, as men tend to be more concerned with outcome factors and women with process factors (Venkatesh and Morris, 2000). Within the context of information privacy and social networking, this could mean that women focus more on the process variables of PMT, like risk perceptions and efficacy, and men are less methodical in the appraisal processes. Gender, in fact, is one factor that has been shown to heavily influence coping strategies (Brems and Johnson, 1989). Therefore, in this study the gender of the social network user was considered as a possible influence on the appraisal processes set forth by PMT.

METHOD

Participants for this study were recruited from an undergraduate MIS course, with course credit offered as an incentive for participation. While social networking websites are popular among college-aged people, and our sample represents that target population (Gordon et al., 1987), social networks also attract a significant number of people outside the age range of 18 to 22. In order to expand our data collection beyond the classroom, we encouraged the students to solicit responses from at least two acquaintances, a technique commonly referred to as "snowball sampling" (e.g., Hochwarter et al., 2003, Peffers and Tuunanen, 2005). This resulted in a more diverse sample than otherwise possible. Overall, we received 307 complete responses from self-reported males, 212 from self-reported females and 3 from subjects who did not indicate their genders. These participants were, at a minimum, registered with at least one social networking website. A control group, described later, included 83 other respondents. The average age of all respondents was 20.6 years, ranging from 18 to 50 years old. The racial/ethnic composition of the sample was 74% U.S. Caucasian, 8.5% international (non-U.S.), 7% Asian-American, 3% U.S. Hispanic, and 2% African-American. Only seven of the respondents reported having children.

Participants visited a website hosted by the authors that consisted of three parts, a pre-intervention survey, the intervention, and a post-intervention survey. The pre-intervention survey collected information on participants' current usage of social networking websites. This was followed by the intervention, the introduction of fear appeal information. The appeal consisted of crime statistics and the accounts of people who had been victimized online, a series of statistics detailing the frequency of online threats, and a list of recommended changes in behavior to help protect one's privacy online. The recommended changes took the form of adaptive responses that subjects could adopt as part of an effort to better protect their personal information. We compiled this information from multiple sources, including the U.S. Department of Justice website, its companion website Cybertipline.com, and a book written by a leading authority on social networking and online safety (Criddle, 2006). The recommended behavioral changes, as well as the other sections of the fear appeal, can be found in the Appendix. To ensure that subjects read the fear appeal in its entirety, the survey required subjects to correctly answer open-ended questions about its content before they could proceed. The post-intervention portion of the survey consisted of measures of the coping strategies and the PMT variables, including perceived threat severity, response costs, response efficacy, and self-efficacy, which are described in the following section. The survey concluded with demographic measures.

Measures

The current study utilized measures found in instruments used in prior research examining PMT which were modified for the context of social networking. The resulting instrument was independently reviewed for appropriate wording by two graduate students who are avid social network users. Modeled after validated PMT measures (Rippetoe and Rogers, 1987), the main dependent variables were the behavioral intentions to respond to the threat information with two maladaptive styles, avoidance and hopelessness, and one adaptive style of coping with the threat information. The avoidance measure consisted of two items, and hopelessness was measured using three items. The measure of intentions to adapt posting behavior was based on the recommended safety guidelines, which advise social network users to refrain from posting personally identifying information on their profiles. In addition, the related variables modeled by PMT were measured using the same context. For example, the response cost of removing one's real name from a profile was captured with an item crafted toward the act of posting personal information ("Removing the personal information from my profile would require a considerable amount of effort"). The associated response efficacy and self-efficacy were measured similarly. Because responses to protection motivation measures, especially those related to the coping appraisal process, can be influenced by social desirability bias, the sequence of the items for the PMT variables was randomized in order to make "appropriate" responses less obvious to subjects (Sheeran and Orbell, 1996).

Additionally, we utilized previously validated items used in past research on online communities to measure the other variables put forth by PMT (see Table 1 below). To measure perceived threat severity, we used a five-item risk assessment measure (Malhotra et al., 2004), which was adapted to capture the risk associated with social networking. The reward factors were measured using seven items from the interest-enjoyment factor of the Intrinsic Motivation Inventory (Deci, 1987) and three items for extrinsic motivation to share with others (Constant et al., 1994).

All of the motivation items were adapted to elicit the rewards gained through use of social networking websites. Finally, fear was measured with one modified item and was used as a manipulation check described in more detail later in this section (Tanner et al., 1991).

Table 1: Item Loadings and Reliabilities of PMT Constructs

Factor/Items	Cronbach's/ Item Loading
Threat Severity	**α =.83**
In general, it is risky to post my personal information on social networking sites.	.83
There would be high potential for loss associated with posting my personal information on social networking sites.	.85
It is uncertain who might be reading my personal information on social networking sites.	.65
Posting my personal information on social networking sites would involve many unexpected problems.	.83
Intrinsic Rewards	**α =.89**
I enjoy sharing my profile with others	.78
Sharing my profile with others is fun to do	.78
Sharing my profile with others is a boring activity (reverse coded)	.82
Sharing my profile with others does not hold my attention at all. (reverse coded)	.76
I would describe sharing my profile with others as interesting	.74
I think sharing my profile with others is quite enjoyable	.76
Extrinsic Rewards	**α =.88**
I earn respect from others by sharing my profile with them.	.86
I feel sharing my profile with others improves my status within my group of friends.	.85
I share my profile with others to improve my reputation.	.82
Self Efficacy	**α =.80**
I have the ability to remove the personal information from my profile.	.81
I have the willpower to remove the personal information from my profile.	.77
Response Efficacy	
Removing the personal information from my profile will help protect me from online dangers.	NA
Response Costs	
Removing the personal information from my profile would require a considerable amount of effort.	NA
Manipulation Check: Fear	
I feel frightened by the potential dangers associated with posting on social networking websites.	NA
Adaptive Response: Intention to Change Risky Behavior	
In the future, I don't intend to post my personal information on my profile.	NA
Maladaptive Response: Avoidance	**α =.83**
I try not to think about the potential dangers associated with social networking websites.	.61
I am not at risk from potential dangers from posting my personal information on social networking websites.	.63
Maladaptive Response: Hopelessness	**α =.79**
There is nothing I can do to avoid the potential dangers associated with posting my personal information on social networking websites.	.72
I feel it is useless to protect myself from the potential dangers associated with social networking websites.	.76
I am at a loss as to how I can protect myself from the potential dangers associated with social networking websites.	.69

Before we could analyze any of the relationships, a confirmatory factor analysis was conducted for factors measured by more than one item[2]. One of the five items measuring risk assessment loaded onto more than one factor, and therefore was dropped from subsequent analyses. All of the extrinsic reward items were retained; however one of the intrinsic reward items cross-loaded onto another factor, and it was also dropped from subsequent analyses. All of the factors demonstrated sufficient reliability with Cronbach's alphas well above 0.7, meeting the minimum requirement suggested by Nunnally and Bernstein (1994). The factors also demonstrated sufficient discriminant validity, as the square root of the AVE (average variance extracted) values for each factor were larger than their correlations with the other factors (see Table 2).

Table 2: Correlation of Constructs, and Square Root of AVE Values (bold in diagonal)

	Items	Mean(SD)	TSA	IM	EM	SE	RE	RC	F	INT	AV	HP
Threat Severity	4	4.4 (1.0)	**.79**									
Intrinsic Rewards	6	4.8 (1.0)	.01	**.78**								
Extrinsic Rewards	3	3.4 (1.3)	.01	.30	**.82**							
Self-Efficacy	2	5.6 (1.1)	.17	.19	-.20	**.82**						
Response Efficacy	1	5.4 (1.2)	.30	.12	-.12	.55	**NA**					
Response Costs	1	2.9 (1.5)	-.02	-.01	.30	-.27	-.14	**NA**				
Fear	1	3.5(1.4)	.40	-.06	.13	-.10	.07	.17	**NA**			
Intent to Change	1	3.8(1.4)	.51	-.14	-.01	.51	.15	.01	.59	**NA**		
Avoidance	2	3.7(1.0)	-.06	.06	.16	-.15	-.19	.15	.04	.01	**.75**	
Hopelessness	3	3.0(1.0)	.03	-.06	.30	-.39	-.28	.36	.34	.16	.43	**.73**

NA = not available

ANALYSIS AND RESULTS

Prior to the main data analysis, we conducted a manipulation check of the fear appeal used as the intervention in this study. The purpose of this manipulation check was to determine if the appeal we used was strong enough to initiate the threat appraisal processes, a check similar to that from the sun tanning example described earlier (McClendon & Prentice-Dunn, 2001). In addition to the 522 subjects who received the fear appeal and provided complete, valid responses to the survey, 83 other subjects completed the instrument without receiving the fear appeal. Internal validity of the manipulation check was addressed by the inclusion of both students and individuals contacted through the snowball sample, which was similar to the larger intervention group. Data collection occurred concurrently for the intervention group and control group. The means for the outcome variables for both the intervention and control groups are displayed in Table 3 below. Two-tailed t-tests indicated that there were significant differences in adaptive and maladaptive intentions between the control and the treatment conditions. Most importantly, the "fear" variable was significant between the intervention and control groups, as fear is considered to be a catalyst for initiating the threat appraisal processes (Norman et al., 2005). The role of fear is supported by the significant differences in all three outcomes (adaptive and maladaptive) between the intervention and control groups, suggesting it did serve to stimulate the appraisal processes. These results suggest that the fear appeal was an effective manipulation for those individuals who received it.

Table 3: Comparison of the Treatment and Control Groups

	Catalyst	**Outcomes**		
	Fear	*Adaptive*: Remove Personal Info	*Maladaptive*: Avoidance	*Maladaptive*: Hopelessness
Intervention (n = 522)	3.48	3.85	3.71	3.02
Control (n = 83)	2.84	2.98	3.07	2.60
Sig (p)	**	**	**	**

** p< .01, * p< .05 Scales ranged from 1(strongly disagree) to 7 (strongly agree).

To test the hypothesized relationships, we conducted three separate hierarchical linear regression analyses, each using one of the three dependent variables (intention to adapt behavior [BI], avoidance, and hopelessness). Hierarchical regression has been used in earlier PMT research (Grothmann and Reusswig, 2006). For these analyses, three responses were dropped because the gender of the respondent was not specified, leaving a sample of 519 social network users. Each regression was conducted using the same three steps. The first step included the control variable of gender, as it had previously been found to have a significant relationship with one of the dependent variables, BI. The second and third steps used the ordering of the appraisal processes observed in the PMT literature (Tanner et al., 1991). Step two added the threat appraisal variables to the model, and step three added the coping appraisal variables. Entering the variables into the analysis in this fashion reflects the temporal priority of the variables; demographic variables can be assumed to be unaffected by other variables in the regression model, and prior literature informed the model as to the chronological order of events (Cohen and Cohen, 1983).

The results of the regression on the adaptive response, BI, are displayed in Table 4 below. Gender was found to be a significant influence on the behavioral intent to remove one's personal information from a social networking profile and, in fact, a post-hoc t-test indicated that females were significantly more likely to do so (females M = 4.15, males M = 3.67; t = -3.73, $p < .001$). The threat appraisal process provided the best explanation for adaptive behaviors, as all three variables in the second step of the regression model had a significant influence on BI. A post-hoc stepwise regression revealed that perceived risk alone explained 25% of the variance in the behavioral intention to adapt one's risky posting behavior, lending support to H1A. None of the coping appraisal variables in the third step, including self-efficacy and response efficacy, were significant, which failed to support H1B and H1C.

Intrinsic rewards were found to have a significant negative effect on users' intentions to remove personal information from their social networking profile, providing support for hypothesis H1D. Extrinsic rewards were not found to have a significant effect on users' intentions to adapt their behavior, failing to support hypothesis H1E. Lastly, response costs did not appear to significantly influence subjects' intentions to adapt their behavior, thus failing to support hypothesis H1F. The next section will present the results of our hypothesis testing for the PMT factors on intentions to continue with the maladaptive behavior.

Table 4: Regression Results for the Adaptive Response

Behavioral Intent to Not Post Personal Info				
Variables	**EV**	**Model 1**	**Model 2**	**Model 3**
Control				
Gender		.16**	.09*	.09*
Threat Appraisal				
Intrinsic Rewards	-		-.15**	-.14**
Extrinsic Rewards	-		.08*	.07
Threat Severity	+		.49**	.48**
Coping Appraisal				
Self-Efficacy	+			-.08
Response Efficacy	+			.08
Response Costs	-			-.01
R^2		.02	.28	.29
Adjusted R^2		.02	.28	.28
ΔR^2		.02**	.26**	.00
F		9.95**	51.62**	30.14**
N		519	519	519

EV = expected valence of the relationship
** p<.01, * p<.05

Hierarchical regression analyses were conducted on the two maladaptive responses, avoidance and hopelessness. The results of the regression analyses are displayed in Table 5 below. Of the hypothesized influences of coping appraisal variables on avoidance, only the perceived response costs of changing one's behavior were significantly associated with the maladaptive behavior. The hypothesized relationships were more prevalent with hopelessness (see Table 5) as, in addition to response costs, both the benefits of intrinsic and extrinsic rewards were significant factors toward the hopelessness response. However, intrinsic rewards were negatively associated with hopelessness, which was opposite of the expectation that it would be a positive influence. The results of both regressions provided full support for H2C and limited support for H2B as extrinsic rewards were significant in predicting hopelessness but not in predicting avoidance.

Additionally, some of the coping appraisal variables had significant influence on maladaptive behaviors, with self-efficacy significantly predicting hopelessness and response efficacy significantly predicting both avoidance and hopelessness, lending partial support for hypothesis H2E and full support for hypothesis H2F. Self-efficacy was the most influential variable for both maladaptive behaviors, explaining 4% of the variance explained for avoidance and 16% for hopelessness. Lastly, perceived risk or threat severity was found to have a significant effect on hopelessness which was in the opposite direction from the hypothesized relationship, failing to support hypothesis H2D. All of the observed results are summarized in Table 6 below. The observed results will be discussed in more detail in the following section and will also be interpreted with respect to other findings.

Table 5: Regression Results for the Maladaptive Responses

		Avoidance			Hopelessness		
Variables	**EV**	**Model 1**	**Model 2**	**Model 3**	**Model 1**	**Model 2**	**Model 3**
Control							
Gender		-.07	-.06	-.03	-.06	-.03	.01
Threat Appraisal							
Intrinsic Rewards	+		.01	.06		-.22**	-.08*
Extrinsic Rewards	+		.15**	.07		.39**	.21**
Threat Severity	-		-.04	.01		.04	.11**
Coping Appraisal							
Self-Efficacy	-			-.04			-.23**
Response Efficacy	-			-.15**			-.12**
Response Costs	+			.10*			.22**
R^2		.01	.03	.07	.01	.13	.28
Adjusted R^2		.01	.02	.06	.01	.13	.27
ΔR^2		.01	.02**	.03**	.01	.13**	.14**
F		2.57	4.13**	5.47**	1.78	20.12**	28.21**
N		519	519	519	519	519	519

EV = expected valence of the relationship
** p<.01 * p<.05

Table 6: Summary of Results

Appraisal/PMT Factors	Adaptive Response	Maladaptive Response – Avoidance	Maladaptive Response – Hopelessness	Supported Hypotheses
Threat Appraisal				
Intrinsic Rewards	Significant	N.S.	Sig./Opposite	H1D
Extrinsic Rewards	N.S.	N.S.	Significant	H2B (Hopelessness only)
Threat Severity	Significant	N.S.	Sig./Opposite	H1A
Coping Appraisal				
Self-Efficacy	N.S.	N.S.	Significant	H2E (Hopelessness only)
Response Efficacy	N.S.	Significant	Significant	H2F
Response Costs	N.S.	Significant	Significant	H2C

DISCUSSION

To summarize the findings, we will first discuss the relationships hypothesized earlier. We found that PMT provides a reasonable explanation of the cognitive processes used by individuals involved in social networking when presented with information that characterizes their behavior as being risky. Consistent with the ordered PMT explanation for the two appraisal processes (Tanner et al., 1991), we found evidence that threat appraisal variables were influential for individuals intending to change their risky behavior. In the full PMT model, with both threat appraisal and coping appraisal variables represented, the perceived risk of threats which could exploit posted personal information was a

heavy influence on the decision to change, overriding any influence of rewards (Floyd et al., 2000). Intrinsic rewards were also a significant negative influence on adaptive BI, suggesting that individuals who find great enjoyment and satisfaction from sharing their profile on social networking websites 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). However, the influence of extrinsic rewards had an unexpected positive influence in the threat appraisal model (Model 2, Table 4) and was not significant in the full PMT model.

As the descriptive statistics displayed in Table 2 show, the respondents reported much more intrinsic motivation to share information with others than extrinsic motivation. That is not surprising; social networking tends to mainly be a voluntary activity for one's personal enjoyment (boyd, 2007). Thoughts of the extrinsic rewards of status and reputation, which were measured in the current study, may be comparatively negligible when deciding to share personal information with others. In fact, in a previous study of information disclosure to commercial websites, extrinsic benefits of status and reputation paled in comparison to preferences of money and time savings (Hui et al., 2006). Although money and time savings are not necessarily relevant to social networking, the earlier finding and the results here suggest that status and reputation, which are tied to social networking, may not be given much credence when deciding whether to post one's personal information.

The gender of the participant was also found to be a significant variable in our model, as it was able to predict those who were more likely to refrain from the risky posting behavior (with women much more likely to do so than men). This may be due in part to the fact that the recommended adaptive behaviors were primarily passive responses, which generally tend to be more attractive to women (Sheehan, 1999), as opposed to adaptive changes that are highly noticeable by others. It may also be partially due to high profile incidents of online abuse and stalking activity that has targeted females, though we consciously included content about victimized males in the fear appeal. Recent research involving PMT and fear appeals suggests that males were most influenced through the use of graphic content (Lennon and Rentfro, 2010), so perhaps a more graphic approach should be taken with regard to social networking threats. Nevertheless, both males and females are clearly targets for identity theft and other social engineering scams involving social networks, so males would be well-advised to pay attention to information detailing potential threats. Finally, none of the coping appraisal variables were found to be significant influences on BI. The ordered PMT model may also explain this result. Those individuals who concluded that the perceived risk of posting personal information was sufficiently dangerous may not have even entered the coping appraisal process. It is possible that self-efficacy, response efficacy, and response costs were not even considered by those considering the adaptive change.

The results were less conclusive for the two maladaptive coping behaviors, particularly for avoidance. Counter to our original predictions, intrinsic and extrinsic rewards did not seem to influence avoidance behavior. In the full PMT model, the response cost (effort) of changing one's risky behavior was the sole hypothesized influence on avoidance behavior. In other words, if an individual perceived the time and effort involved with removing his or her personal information as being more onerous than the consequences of the threat itself, he or she was more likely to engage in avoidance. PMT more fully explained the coping process leading to hopelessness than avoidance. An explanation for the difference between these maladaptive responses could be that avoidance is caused by a premature inhibition of cognitive processing, whereas hopelessness does take external factors into consideration (Hayes et al., 2005). While both maladaptive behaviors result in the continuance of risky behavior, individuals behaving due to avoidance may not fully process the PMT variables when choosing to ignore threat information, as opposed to individuals engaging in hopelessness, who at least perform the threat appraisal process before deciding that the threat is inevitable.

Of the hypothesized relationships, extrinsic rewards and response costs both significantly influenced hopelessness responses. As is modeled by PMT, the importance of extrinsic rewards increases the likelihood that individuals will continue the risky behavior that results in those rewards, rather than adopt a more protective behavior. Again, individuals who respond with hopelessness at least conduct the threat appraisal process, of which extrinsic rewards are a key part. Intrinsic rewards were also significant predictors of hopelessness, but in the opposite direction from what was hypothesized. Instead of the enjoyment associated with social networking being a positive influence toward a hopeless response in the face of online threats (resulting in the continued risky behavior), it was negatively associated with hopelessness. In other words, the higher the perceived intrinsic benefits derived from social networking, the less likely the individual is to respond to threats with hopelessness. The role of intrinsic motivation in PMT has been mixed (Floyd et al., 2000) and is often not represented in analyses (Milne et al., 2000), providing grounds for future research. Although this is purely speculative, the hedonic nature of and the enjoyment gained from social networking may simply be a stronger value for users than fear. Similar results occurred in a study on the dangers of sun tanning (Leary and Jones, 1993), in which people who were dispositionally high in concern for their personal 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. Our social networking users may have noted the potential danger caused by posting one's personal information online, but perhaps the enjoyment from being able to display that information is believed to be worth the risk.

Likewise, response efficacy was negatively associated with both avoidance and hopelessness; individuals who believed the suggested behavioral change would be ineffective against online threats were more likely to engage in one of the maladaptive behaviors. Finally, the individual's self-efficacy, the belief in his or her ability and willpower to make the recommended behavioral changes, also negatively influenced hopelessness. This lends support to earlier reports that many users simply do not understand how to use methods provided for protection, or do not believe they are even capable of enacting them, so they respond with indifference (Paine et al., 2007).

While the majority of the existing IS literature utilizing PMT has dealt primarily with network security issues (e.g. users deciding to comply with security policies, users intending to take preventive actions against spyware threats) (Johnston and Warkentin, 2010), this study has introduced PMT into the realm of personal information privacy. It could thus be argued that the current study involves risky behavior at a more personal level for the individual engaging in the risk assessment. In the earlier IS PMT studies, the organization is frequently described as being vulnerable to the individual's risky behavior (Herath and Rao, 2009), but here the individual is the lone party threatened with losses resulting from the risky behavior. Therefore, a maladaptive response to online threats that have direct personal implications would seem to be a more personal decision, so the number of people in this study who responded with avoidance or hopelessness is disconcerting. While we strongly suggest that future studies account for the possibility of a maladaptive response, a potential future direction for PMT studies in the field of information systems could add an individual's perceptions of the entities that are vulnerable to the threat of interest to the model, in the hopes of determining whether variables like organizational commitment and self-preservation differ with changes in those perceptions.

Implications, Limitations, and Future Research

This work has implications for research not only utilizing PMT, but for computer-mediated communication (CMC) as well. This study adapts PMT within a computer-mediated context, and the theory seems to have some potential explanatory power for risky self-disclosure behavior in CMC contexts. Previous PMT research has speculated on more effective methods of presenting threat information to individuals, including fear appeal efforts across time intervals (McClendon and Prentice-Dunn, 2001) and designing information to focus more on motivating recipients than on merely reporting facts (Prentice-Dunn et al., 1997). The fear appeal used in this study attempted to remedy the latter by not only reporting statistics on online threats, but also the news accounts of individual victims. This study also presents additional evidence that PMT provides an explanation for the risky behavior of users online, and our results further establish the relevance of PMT in the arena of information systems research. Additionally, this study provides insight into maladaptive responses, and has analyzed PMT data in a time-ordered sequence that, to our knowledge, has not been explored in IS research and has seldom been explored elsewhere. In a recent discussion about technology threat avoidance, Liang and Xue (2009) noted that a distinction must be made between the avoidance of malicious technology (a maladaptive behavior) and the adoption of safeguarding technology (an adaptive behavior); while the two behaviors may outwardly provide the same protective results, they are motivated by two different appraisals, an "avoidance-approach" mechanism. The current study provides supporting evidence that such a distinction exists, and the appraisal processes that lead to one behavior or the other need to be more fully understood by researchers and managers.

For practitioners, the results offer insights for educating social networking users on the dangers and the countermeasures to protect one's personal information. A majority of respondents to one survey were clearly uncomfortable with the addition of a push-based information release to at least one social networking website, primarily because it appeared to take control away from users (Hoadley et al., 2010). The website stated publicly that the "News Feed" information release was accessible by friends only, but users demanded the control mechanisms be reverted back to their earlier state. The website complied, but users were no more safe than before (Hoadley et al., 2010). The "News Feed" incident points to how drastic administrative changes affect the complacency that many social network users have toward information privacy, even when there is not a true effect on privacy itself. While the administrators of social networking websites have a responsibility to protect their users' information, their efforts are likely best served by targeting the main factor identified in this study that encourages adaptive behavioral change: the perceptions of threats to information privacy. As mentioned in the introduction, the best policy about posting personal information is to not post it to begin with.

One of the limitations of this study involves the snowball sampling effort and the age of the participants who provided responses to the survey. While we made a conscious effort to solicit responses from people older than the traditional college student, the average age of the participants was 20.6 years. The students we originally recruited to find additional participants may have had difficulty finding older social networking users. Correlational analyses of the demographic variables with the outcome variables did not indicate that age influenced the behavioral intentions of social networking users, but as the age range of users becomes wider with time, the influence of age on protection motivation should be revisited. For the time being, the generalizability of these results may be limited.

Another limitation to the results is related to the inability to predict the amount of behavioral change that will actually occur. Consistent with other IS research and earlier protection motivation research, we measured behavioral

intentions, which does not permit definitive predictions about participants' actions (Ho et al., 2005). The findings in this study should be considered with these limitations in mind. Also, the measures used for certain PMT variables, including fear, consisted of a single item. Single-item measures are appropriate if the construct being measured is narrow and unambiguous to subjects (Sackett and Larson, 1990). Many PMT studies have successfully employed single-item measures in the past (Norman et al., 2005, Orbell and Sheeran, 1998). Given the context provided to the subjects by the survey instructions, we believe these measures were appropriate for the current study. However, we hope future researchers will provide further support by investigating our hypotheses utilizing multiple-item measures for the constructs.

CONCLUSION

This study investigated the process of protection motivation in response to potential threats involving social networking websites. As mentioned earlier, the popular press is rife with stories of social networking users who have been victimized by predators who have access to their personal information. In fact, recent reports suggest that cyberstalking is now more prevalent than real-world stalking. The majority of victims reported being victimized on social networking sites, suggesting that these predators now make social networking sites their primary target (Huffington Post, 2011). For that reason alone, it is important to investigate effective ways of protecting social network users from potential online dangers.

The results of our study indicate that some people, particularly females, do take information about online threats seriously, and are at least willing to consider adaptive behavioral responses meant to protect them. This result is encouraging, as women are more likely to be targeted by online predators, but men are mistaken if they believe themselves to be immune from being victimized. One other reason for optimism is that social cognitions like those modeled by PMT are not known to be enduring (Ben-Ahron et al., 1995). Thus, there are opportunities to inform users and encourage adaptive behaviors, even with those users who currently maintain risky behavior.

Social networking will continue to exist in one form or another for time to come. The popularity of certain networking websites may fluctuate, but the enjoyment and social satisfaction gained from participating in online social networking will likely remain high for many people. This means that the personal information that users enjoy sharing will also be at risk. We should not be satisfied until all users of social networking websites seriously consider the information they post and communicate to others.

REFERENCES

Abraham, C., P. Sheeran, D. Abrams, and R. Spears (1994) "Exploring Teenagers' Adaptive and Maladaptive Thinking In Relation to the Threat of HIV Infection," *Psychology and Health* (9), pp. 253-272.

Acquisti, A. and R. Gross. (2006) Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. Paper presented at the *Sixth Workshop on Privacy Enhancing Technologies,* Cambridge, UK, June 28-30, 2006.

Barak, A. and W. Fisher (2002) The Future of Internet Sexuality, in A. Cooper (Ed.) *Sex and the Internet: A Guidebook for Clinicians*, New York, NY: Brunner-Routledge, pp. 267-280.

Ben-Ahron, V., D. White, and K. Phillips (1995) "Encouraging Drinking at Safe Limits on Single Occasions: The Potential Contribution of Protection Motivation Theory," *Alcohol & Alcoholism* (30) 5, pp. 633-639.

Boss, S. and D. Galletta (2008) "Scared Straight: An Empirical Comparison of Two Major Theoretical Models Explaining User Backups," Paper presented at the *Ninth International Research Symposium on Accounting Information Systems*, *Paris*, France, December 13, 2008.

Boyd, D. (2007) Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life, in D. Buckingham (Ed.) *MacArthur Foundation Series on Digital Learning*, Cambridge, MA: MIT Press.

Boyd, D. and N. Ellison (2007) "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication* (13) 1, pp. 210-230.

Brems, C. and M. E. Johnson (1989) "Problem-Solving Appraisal and Coping Style - The Influence of Sex-Role Orientation and Gender," *Journal of Psychology* (123) 2, pp. 187-194.

Byrnes, J., D. Miller, and W. Schafer (1999) "Gender Differences in Risk Taking: A Meta-analysis," *Psychological Bulletin* (125) 3, pp. 367-383.

Cohen, J. and P. Cohen (1983) *Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences*. Hillsdale, N.J.: Lawrence Erlbaum Associates, Inc.

Constant, D., S. Kiesler, and L. Sproull (1994) "What's Mine is Ours, or is it? A Study of Attitudes about Information Sharing," *Information Systems Research* (5) 4, pp. 400-421.

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

Deci, E. L. (1987) "Theories and Paradigms, Constructs and Operations - Intrinsic Motivation Research is Already Exciting," *Journal of Social Behavior and Personality* (2) 2, pp. 177-185.

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

Fruin, D., C. Pratt, and N. Owen (1991) "Protection Motivation Theory and Adolescents' Perceptions of Exercise," *Journal of Applied Social Psychology* (22) 1, pp. 55-69.

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

Gibbs, J., N. Ellison, and R. Heino (2006) "Self-Presentation in Online Personals: The Role of Anticipated Future Interaction, Self-disclosure, and Perceived Success in Internet Dating," *Communication Research* (33) 2, pp. 152-177.

Gordon, M., L. Slade, and N. Schmitt (1987) "Student Guinea Pigs: Porcine Predictors and Particularist Phenomena," *Academy of Management Journal* (12) 1, pp. 160-163.

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

Gustafson, P. (1998) "Gender Differences in Risk Perception: Theoretical and Methodological Perspectives," *Risk Analysis* (18) 6, pp. 805-811.

Hayes, A. M., C. G. Beevers, G. C. Feldman, J. Laurenceau, and C. Perlman (2005) "Avoidance and Processing as Predictors of Symptom Change and Positive Growth in an Integrative Therapy for Depression," *International Journal of Behavioral Medicine* (12) 2, pp. 111-122.

Herath, T. and H. R. Rao (2009) "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations," *European Journal of Information Systems* (18), pp. 106-125.

Ho, R., G. Davidson, and V. Ghea (2005) "Motives for the Adoption of Protective Health Behaviors for Men and Women: An Evaluation of the Psychosocial-appraisal Health Model," *Journal of Health Psychology* (10) 3, pp. 373-395.

Hoadley, C., H. Xu, J. Lee, and M. B. Rosson (2010) "Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry," *Electronic Commerce Research and Applications* (9) 1, pp. 50-60.

Hochwarter, W., C. Kacmar, P. L. Perrewe, and D. Johnson (2003) "Perceived Organizational Support as a Mediator of the Relationship between Politics Perceptions and Work Outcomes: A Multi-level Analysis," *Journal of Vocational Behavior* (63), pp. 438-456.

Huffington Post (2011) “Cyberstalkers Take To Social Networks Over Dating Sites,” Retrieved on April 11, 2011, from http://www.huffingtonpost.com/2011/04/11/cyberstalking-study-social-network_n_847037.html

Hui, K., B. Tan, and C. Goh (2006) "Online Information Disclosure: Motivators and Measurements," *ACM Transactions on Internet Technology* (6) 4, pp. 415-441.

Jianakoplos, N. and A. Bernasek (1998) "Are Women More Risk Averse?" *Economic Inquiry* (36) 4, pp. 620-630.

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

Lazarus, R. (1991) "Cognition and Motivation in Emotion," *American Psychologist* (46), pp. 352-367.

Leary, M. and J. Jones (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, pp. 1390-1406.

Lee, D., R. LaRose, and N. Rifon (2008) "Keeping Our Network Safe: A Model of Online Safety Behaviour," *Behaviour & Information Technology* (27) 5, pp. 445-454.

Lennon, R. and R. Rentfro (2010) "Are Young Adults Fear Appeal Effectiveness Ratings Explained by Fear Arousal, Perceived Threat and Perceived Efficacy?" *Innovative Marketing* (6) 1, pp. 58-65.

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

Maddux, J. (1993) "Social Cognitive Models of Health and Exercise Behavior: An Induction and Review of Conceptual Issues," *Journal of Applied Sport Psychology* (5), pp. 116-140.

Maddux, J. and R. Rogers (1983) "Protection Motivation Theory and Self-efficacy: A Revised Theory of Fear Appeals and Attitude Change," *Journal of Experimental Social Psychology* (19), pp. 242-253.

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

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

McMath, B. F. and S. Prentice-Dunn (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, pp. 621-643.

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

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

Mulilis, J. and R. Lippa (1990) "Behavior Changes in Earthquake Preparedness Due to Negative Threat Appeals: A Test of Protection Motivation Theory," *Journal of Applied Social Psychology* (20), pp. 619-638.

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

Norman, P., H. Boer, and E. Seydel (2005) Protection Motivation Theory, in M. Conner and P. Norman (Eds.) *Predicting Health Behavior: Research and Practice with Social-Cognition Models*, Buckingham: Open University Press, pp. 81-126.

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

Orbell, S. and P. Sheeran (1998) "'Inclined Abstainers': A Problem for Predicting Health-related Behaviour," *British Journal of Social Psychology* (37), pp. 151-165.

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

Paine, C., U. Reips, S. Stieger, A. Joinson, and T. Buchanan (2007) "Internet Users' Perceptions of 'Privacy Concerns' and 'Privacy Actions'," *International Journal of Human-Computer Studies* (65) 6, pp. 526-536.

Peffers, K. and T. Tuunanen (2005) "Planning for IS Applications: A Practical, Information Theoretical Method and Case Study in Mobile Financial Services," *Information & Management* (42) 3, pp. 483-501.

Prentice-Dunn, S., J. Jones, and D. Floyd (1997) "Persuasive Appeals and the Reduction of Skin Cancer Risk: The Roles of Appearance Concern, Perceived Benefits of a Tan, and Efficacy Information," *Journal of Applied Social Psychology* (27) 12, pp. 1041-1047.

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

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

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

Rosenblum, D. (2007) "What Anyone Can Know - The Privacy Risks of Social Networking Sites," *IEEE Security & Privacy* (5) 3, pp. 40-49.

Sackett, P. and J. Larson (1990) Research Strategies and Tactics in Industrial and Organizational Psychology, in M. D. Dunnette and L. M. Hough (Eds.) *Handbook of Industrial and Organizational Psychology*, Palo Alto, CA: Consulting Psychologists, pp. 419-489.

Sandvine.com (2011) "Global Internet Phenomena Report: Spring 2011." Retrieved September 8, 2011, from http://www.wired.com/images_blogs/epicenter/2011/05/SandvineGlobalInternetSpringReport2011.pdf.

Schau, H. J. and M. Gilly (2003) "We Are What We Post? Self-presentation in Personal Web Space," *Journal of Consumer Research* (30) 3, pp. 385-404.

Seydel, E., E. Taal, and O. Weigman (1990) "Risk Appraisal, Outcome, and Self-efficacy Expectancies: Cognitive Factors in Preventive Behavior Related to Cancer," *Psychology and Health* (4) 2, pp. 99-109.

Sheehan, K. B. (1999) "An Investigation of Gender Differences in Online Privacy Concerns and Resultant Behaviors," *Journal of Interactive Marketing* (13) 4, pp. 24-38.

Sheeran, P. and S. Orbell (1996) "How Confidently Can We Infer Health Beliefs from Questionnaire Responses?" *Psychology and Health* (11), pp. 273-290.

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

Socialnomics.net (2011) "Social Network User Statistics." Retrieved September 8, 2011, from http://www.socialnomics.net/2011/08/16/social-network-users-statistics/.

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

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

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

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, pp. 20-36.

Valkenburg, P., J. Peter, and A. Schouten (2006) "Friend Networking Sites and Their Relationship to Adolescents' Well-being and Social Self-esteem," *CyberPsychology & Behavior* (9) 5, pp. 584-590.

Venkatesh, V. and M. G. Morris (2000) "Why Don't Men Ever Stop to Ask for Directions? Gender, Social Influence, and Their Role in Technology Acceptance and Usage Behavior," *MIS Quarterly* (24) 1, pp. 115-139.

Wanous, J., A. Reichers, and M. Hudy (1997) "Overall Job Satisfaction: How Good are Single-Item Measures?" *Journal of Applied Psychology* (82) 2, pp. 247-252.

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

Wolak, J., D. Finkelhor, and K. Mitchell (2004) "Internet-initiated Sex Crimes against Minors: Implications for Prevention Based on Findings from a National Study," *Journal of Adolescent Health* (35) 5, pp. 424-433.

[1] http://www.sophos.com/pressoffice/news/articles/2009/12/facebook.html, last accessed 2/13/2010

[2] Single-item measures were adopted to assess some of the constructs under study. We acknowledge that this practice may lead to potential problems, especially when measuring complex, multidimensional constructs. However, studies have shown that single-item measures are acceptable when measuring narrow, unambiguous concepts (Wanous, Reichers, and Hudy, 1997). Additionally, many PMT studies have successfully employed single-item measures in the past (Norman et al., 2005, Orbell and Sheeran, 1998).

APPENDIX: FEAR APPEAL WITH THREAT INFORMATION

You should be aware of potential online dangers on social networking websites and what kind of threats they can present.
The following are cases reported by the US Department of Justice.

- A security guard in Los Angeles targeted a woman who had earlier rejected his romantic advances by posting her home phone number and home address on Internet forums and websites. The victim received several unsolicited phone calls and visits from strangers at her residence. The security guard was sentenced to six years in prison.
- In May of 2007, MySpace turned over the names of 245 registered sex offenders who were using their site to the North Carolina Attorney General's office.
- From *The Washington Post*: The FBI last month warned MySpace users of a phony bulletin post urging people to click on a link to "check out old school pictures." A virus seeking financial information recently invaded Orkut, Google's social networking site. Early last month, unsolicited instant messages attempted to lure MySpace users into divulging account information, and about a dozen other sites that spoof the MySpace log-in page have been discovered.
- From *The Mirror*: Lara Coton knows about the dangers of putting photos on the net. The 17-year-old from Tamworth submitted an innocent family photograph to an art website but was horrified to discover it had been used on the cover of an X-rated movie.

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.

- One in five children aged 12 to 17 are sexually solicited online every year in the United States, and a similar number is estimated in the United Kingdom.
- Contrary to common belief, not all online victims are female. 25 percent of reported victims are male.
- 23 percent of online victims of Internet sex crimes and cyberstalking were between the ages of 18 to 25.
- One major Internet Service Provider receives approximately 15 complaints per month of cyberstalking, in comparison to virtually no complaints of cyberstalking just one or two years ago. (US Department of Justice)
- In a recent study, forty percent of the respondents had been threatened or sent abusive messages via instant message, chat room, discussion forums, and networking sites. (Paul Bocij, firstmonday.com)
- The FBI's Internet Crime Complaint Center logged its 1 millionth complaint on July 11, 2007. (FBI)

Finally, you should also be aware of possible ways to protect yourself and your identity 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*:

- Never post your personal information, such as your name, cell phone number, address, or the name of your school or school team.
- Never give out your password to anyone.
- Only add people as friends to your site if you know them in person.
- Never meet in person with anyone you first "met" on a social networking site. Some people may not be who they say they are.
- Think before posting your photos. Personal photos should not have revealing information, such as school names or locations. Look at the backgrounds of the pictures to make sure you are not giving out any identifying information without realizing it. The name of a mall, the license plate of your car, signs, or the name of your sports team on your jersey all contain information that can reveal your location. And never post sexually provocative photos of yourself or your friends.
- 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.
- Remember that posting information about your friends could put them at risk. Protect your friends by not posting any names, passwords, ages, phone numbers, school names, or locations. Refrain from making or posting plans and activities on your site.

ABOUT THE AUTHORS

Kent Marett is an Assistant Professor of Business Information Systems at Mississippi State University. He received his Ph.D. in Management Information Systems from Florida State University. His research is primarily focused on online deceptive communication, information security, the use of technology by work groups, and human-computer interaction. His research has been published in several leading journals, including the *Journal of Management Information Systems*, *Journal of the AIS*, *IEEE Transactions on Professional Communication,* and *Journal of Applied Social Psychology*.

Anna L. McNab is an Assistant Professor in the College of Business Administration at Niagara University. She received her Ph.D. from Washington State University with an emphasis in Information Systems. She also holds an undergraduate degree in Business Administration double-majoring in MIS and Operations Management and a M.B.A. degree both from Washington State University. Her research interests include human-computer interaction, user acceptance of information systems, motivations of joining online communities and examination of methods used in IS research. Dr. McNab's research has appeared in journals such as *The DATA BASE for Advances in Information Systems*, *AIS Transactions on Human-Computer Interaction*, *Journal of Organizational Computing and Electronic Commerce*, and *BRC Business Educational Journal* as well as in the Proceedings of the International Conference on Information Systems, Americas Conference on Information Systems and the DSI Annual Meeting.

Ranida B. Harris is an Associate Professor of Management Information Systems at Indiana University Southeast. She received her Ph.D. in Management Information Systems from Florida State University. Her research interests include the effects of computer technologies on communication, performance, and decision making. Her publications appear in *Journal of Applied Social Psychology, Journal of Social Psychology, Journal of Managerial Issues, Journal of Behavioral and Applied Management, Journal of Organizational and End User Computing, Information Systems Education Journal,* and other journals. Dr. Harris's teaching interests include business computer applications, systems analysis and design, and database management systems.

ISSN: 1944-3900

Transactions on Human-Computer Interaction