User Behavior on Online Social Networks and the Internet: A Protection Motivation Perspective

by

Tziporah Stern

A dissertation submitted to the Graduate Faculty in Business in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York.

2011

This manuscript has been read and accepted for the
Graduate Faculty in Business in satisfaction of the
dissertation requirement for the degree of Doctor of Philosophy.

Nanda Kumar

Date | Chair of Examining Committee

Joseph Weintrop

Date | Executive Officer

Martin Frankel

Linda Friedman

Supervisory Committee

THE CITY UNIVERSITY OF NEW YORK

ABSTRACT

User Behavior on Online Social Networks and the Internet: A Protection Motivation Perspective

by

Tziporah Stern

Advisor: Dr. Nanda Kumar

The advent of the Internet and the digital society has heralded concerns about potential for privacy loss. While past research has delved into aspects of individuals' privacy concerns, research on online social networks (such as Facebook) consistently shows that people disclose a vast amount of private information voluntarily and seemingly without reserve. In order to examine disclosure and protection behavior, this research draws on Protection Motivation Theory (PMT) and Social Exchange Theory (SET) to build a model examining these behaviors specifically in the Online Social Networks (OSN) setting. A survey was conducted which confirmed that vulnerability, severity, trust, and privacy disposition were all antecedents to perceived privacy risk in this context. In addition, this research also showed the mediating role played by PMT variables - benefits, risk, and efficacy - on both maladaptive behavior *and* protection behavior.

A second study triangulated these findings by manipulating threat and response efficacy in a 2 x 2 experimental design to further examine their role in maladaptive behavior and protection behavior. This study drew on the Extended Parallel Process Model (EPPM), an extension of PMT, and investigated whether fear about ID threat is a necessary condition for *any* response to occur (regardless of whether the response is maladaptive or adaptive). The results confirmed EPPM suppositions in that the group with the highest intention to protect itself was the group in the high threat high efficacy condition. Both threat and efficacy had a main effect on the

dependent variables indicating that either threat *or* efficacy was a sufficient condition to initiate a response.

This research also conducted a third study to test the impact of better visual representation of privacy settings on an OSN. A color-coded wheel interface was designed to simultaneously display, not only user settings, but also recommended ('safe') settings. This research drew on Cognitive Fit (CF) theory and compared the new interface to the tabular interface currently used by Facebook. This experiment confirmed the basic tenets of CF theory and found that the wheel interface was more enjoyable and was superior in the comprehension of complex information.

This research bolsters privacy research by using an experimental design in conjunction with a survey to triangulate findings regarding protection behavior. It successfully applies Protection Motivation Theory in the IS context and manipulates the PMT variables in a way not previously accomplished in IS. It also explores the use of different interfaces for privacy settings on an OSN by designing and testing a superior interface for privacy settings.

ACKNOWLEDGEMENTS

This work is dedicated to my father-in-law, Dr. Andrew Stern, who passed away while I was working on this dissertation. He was the true embodiment of a "scholar and a gentleman." His scholarship and unquenchable thirst for knowledge in all its forms continues to inspire and inform my own intellectual pursuits.

I would like to express my profound appreciation to Dr. Nanda Kumar, my advisor and chair of my dissertation committee, whose advice and guidance, at all hours, were invaluable every step of the way. I also wish to thank Dr. Linda Friedman and Dr. Martin Frankel for serving on my committee and providing thoughtful comments and offering helpful suggestions. My sincerest appreciation to Dr. Marios Koufaris for the opportunity to collaborate on a number of research projects, and who along with Dr. Joseph Weintrop assisted me towards completing the doctoral program requirements. I am also grateful to Dr. Raquel Benbunan-Fich for her assistance in recruiting subjects for my study.

Thank you to my parents for all the support they have given me, not only while I worked towards my doctorate degree, but throughout my life. To my mother-in-law, Dr. Rachel Stern, thank you for your assistance in providing another set of eyes to look over the children and this dissertation. Last but not least, to my husband who was a constant source of encouragement throughout this dissertation as well as my academic career.

List of Tables

List of Figures

Chapter 1

INTRODUCTION

In the past few years, Online Social Networks (OSN) such as Facebook and MySpace, have been attracting millions of users around the world. People are joining online social networks to build communities with shared interests, share information with their friends (and even strangers), and to chat, blog, message, and share pictures. Online social networks have become an intrinsic part of our lives which has been made possible with the digitalization of information and the rapid growth of technology. However, as with any new technology there are always underlying factors to consider. With the advent of the Internet, the digitalization of information, and its ease of access, privacy concerns are pushed to the forefront. Online social networking actually exasperates the privacy problem since individuals voluntarily disclose information without any regard as to the sensitivity of the information and to whom it is being disclosed.

In order to understand why people disclose so much information, and seem to leave themselves unprotected it is important to have insight into the underlying motivations for disclosure and protection on Online Social Networks. It is also important to determine what causes this disclosure and if changes in perceptions or in the interface used have an effect on disclosure and protection. This paper uses Protection Motivation Theory and Social Exchange Theory to delve into the intentions of individuals when they use Online Social Networks. It also uses Cognitive Fit Theory to understand comprehension of privacy settings. The paper is organized as follows: first a brief introduction to privacy and online social networks will be explored; next the research question and model will be presented. Then, an in-depth literature review will be followed by theory and hypothesis development. The methodology section is presented next and is split into

three different sections, one for each study conducted. Last, the conclusion summarizes the results from all three studies and suggests areas for future research.

1.1 Privacy Background

Privacy is an intrinsic right people have and has been the subject of much philosophical literature such as Aristotle and Locke (DeCew 2006). In fact, the Universal Declaration of Human Rights adopted by the General Assembly of the United Nations states ,"No one shall be subjected to arbitrary interference with his privacy" (1948). Privacy can be defined as, "the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves" (Smith 2000; p6). It is also considered, "an interpersonal boundary process by which a person or group regulates interaction with others" (Altman 1975; p6). Similarly, in a seminal paper about privacy Warren and Brandeis (1890) define privacy as, "the right to be let alone" (p195). When describing privacy in this fashion, Warren and Brandeis refer to the fact that innovations in technology, such as instant photography that makes the circulation of pictures in newspapers easier, creates new needs for new laws to address the individual's right to privacy. Their article's purpose was more geared towards public policy, yet, the question remains the same even now, 120 years later: What is privacy, what rights does it encompass, and, more importantly, how does technology change the concerns?

Privacy can be divided into four overlapping concepts (Epic 2003):

- Information privacy - relating to handling of personal data
- Bodily privacy - physical person
- Privacy of communications – i.e. mail, phone, e-mail

- Territorial privacy - private versus public space.

This dissertation studies the first dimension of privacy, or information privacy. A comprehensive definition of information privacy[1] can be obtained by combining the various views and identifying the common theme, which is control. In other words, privacy is an individual's right to *control (a)* who has information about them, *(b*) what information is collected, and *(c)* how information about them is disseminated. This viewpoint is a seminal definition of privacy and is drawn on by many authors. For example, Westin (1967), in an influential book described by Fraenkel (1968) as, "so comprehensive that there should be no need for any work of this kind in the calculable future" (p196), defined privacy as, "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent, information about them is communicated to others" (Westin 1967; p7). Another similar definition is "management of communication" or the right of individuals to communicate when they want to (Bennett 1967; p371). Privacy is also referred to as, "the ability of the individual to control personal information about one's self" (Stone et al. 1983; p160), the "capability to determine what one wants to reveal and how accessible one wants to be" (Bellotti 1997; p89), and "selective control of access to the self" (Altman 1975; p18). This core definition, one of control (Altman 1975, Kelvin 1973, Johnson 1974), has not changed even now with the many rapid changes in technology, although each new technology brings forth new questions of people's rights.

Today, in the information age, the digitization of many types of information makes the privacy issue very important. With the rapid advances in technology, retrieval of a specific records is quicker (Masuda 1979, Peterson 1995); copying, transporting, collecting, storing, integrating and

[1] From this point forward all instances of privacy refer to information privacy

processing large amounts of information is easier (Graham 1987, Masuda 1979, Nisenoff et al. 1979, Peterson 1995). In addition, with the advent of the Internet and community networking, the *magnitude* of information available has increased exponentially (Weston 1997). Because of this huge increase of information available and the development of search engines to make information collection easier, individuals are now easily capable of accessing many different information directories (Aljifri and Navarro 2004, Gindin 1997, Strauss and Rogerson 2002). This ease of access potentially leads to the exploitation of techniques such as data mining. Using data mining, information can be extracted from large databases and analyzed from many different perspectives to find patterns in data. It can also use identifying information to extract many pieces of information from different databases which creates new information from data that may have originally been meaningless and hence violate a person's right to privacy (Graham 1987, Tavani 1999, Tuerkheimer 1993).

Information privacy becomes applicable in many different situations. For example, there are extensive streams of research on privacy and peoples' rights in the healthcare industry with regard to sensitive medical information (Collins 2007, Glenn 2000, Grover et al. 1998, Kelly and Unsal 2002, O'Brien and Yasnoff 1999, Rindfleisch 1997), on employees rights to privacy while in the workplace (Eddy et al. 1999, Grover et al. 1998, Oliver 2002, Sipior and Ward 1995, Weisband and Reinig 1995), and on the most general level, on citizens rights to privacy from government intrusion and surveillance (Davis 2005, Otjacques et al. 2007). Additionally, with changes in technology there are added concerns and more potential for privacy breaches. For example: digitization of information makes accessing private healthcare records easier (Rindfleisch 1997); e-mail, a huge technological breakthrough, creates new questions of

employers' rights to read their employees' e-mail (Oliver 2002); and last, digitization of government records, creates concerns regarding ease of access (Davis 2005, Belanger and Hiller 2006), cross-referencing between online and offline databases, and the magnitude of information collected as well as the security measures in place to protect it (Belanger and Hiller 2006).

1.2 Privacy Concerns

The Internet exacerbates the privacy problem since it is a vehicle for information collection which can be collected explicitly or implicitly. The key difference is knowledge or *awareness* of collection and a conscious decision to disclose. Explicit data is willingly disclosed by the individual (i.e. via forms) while implicit data is collected secretly and the individual has limited or no knowledge of its collection. There are many different types of data collected electronically and digitized and this leads to privacy concerns regarding its disclosure. The way information is collected is also of concern to individuals. For example, new technologies incorporated in the Internet, such as cookies, search engines, web cameras, spyware, and targeted ads have clear privacy infringement problems.

Research has been addressing the many new causes for concern when using new technology and has identified four main concerns: collection, errors, secondary use, and improper access (Smith et al. 1996). A good part of the literature addresses these concerns since Smith et al. (1996) created and validated an instrument for measuring them. Occasionally, authors will use different words to describe the same concern, or discuss a specific instance of a concern. In Table 1: Information Concerns, some specific instances have been grouped into the four main categories Smith et al. (1996) have identified.

- *Access* refers to the fact that information may be readily available to people who are unauthorized to access it. In particular, individuals are concerned with who actually has access and if the data will be sold or used by third parties (Hoffman 2003, Cranor et al. 1999, Hine and Eve 1998).
- *Collection* is the concern that such a vast array of information is being collected and stored in databases. Individuals want to know the kind of information collected (Hoffman 2003, Cranor et al. 1999, Hine and Eve 1998).
- *Errors* refer to the concern that information that is collected is inaccurate.
- *Use* is the concern of the purpose for which information is collected (Hine and Eve 1998, Cranor et al. 1999, Tavani 1999, Hoffman 2003). Individuals are concerned that information will be collected for one reason and used for another. For example, a business selling its customer database is a classic example of secondary use of data.

Individuals do not want to share information just to be hassled by marketing calls or for advertising purposes (Hine and Eve 1998). They are also concerned about computer merging and matching since they may have authorized data for one purpose but not for another and through data mining techniques this information is extracted for further use and analysis (Tavani 1999), which may lead to price (Danna and Gandy 2002, Odlyzko 2003) and market discrimination (Graham 1987, Danna and Gandy 2002).

While the above classification has been developed into a general scale for privacy concern, another popular classification of users concerns, geared towards *online* concerns, identifies three main concerns (Malhotra et al. 2004):

Table 1: Information Concerns

Concern			**Reference**
Access:	(in general)		Cranor et al. 1999; Smith et al. 1996; Stewart and Segars 2002; Smith 1993; Berghel 2000; Hoffman 2003, Paine et al. 2007
	Intrusion	Video surveillance on the Internet	Meeks 1997
		Web Bugs	Hale 2001
		Spam	Wang et al. 1998; Hoffman 2003; Kling et al. 1999, Paine et al. 2007
		Spyware	Paine et al. 2007, Gibson, 2005; Shukla and Nah, 2005; Warkentin et al. 2005
Collection :	(in general)		Smith et al. 1996; Smith 1993; Strauss and Rogerson 2002; Hoffman 2003; Kirsh et al. 1996; Campbell 1997; Lopez 1994; Kelly and Unsal 2002; Rohme and Milne 2004
	Storage		Strauss and Rogerson 2002; Kirsh et al. 1996; Lopez 1994
Errors:			Smith et al. 1996; Stewart and Segars 2002; Smith 1993; Peterson 1995; Gindin 1997; Campbell 1997
Use:	(in general)		Hoffman 2003; Cranor et al. 1999; Campbell 1997; Tavani 1999; Hine and Eve 1998; Kirsh et al 1996; Gindin 1997; Lopez 1994; Rohme and Milne 2004
	Creating marketing profiles of consumers		Culnan and Armstrong 1999
	Cross matching		Lewis 1988; Tavani 1999; Peterson 1995; Lopez 1994
	Distributing and Sharing		Strauss and Rogerson 2002; Smith 1993; Cranor et al. 1999; Miyazaki and Fernandez 2001; Grupe 1995 (resale)
	Analyzing		Strauss and Rogerson 2002
	Improper Use:	Identity Theft	Berghel 2000; de George 1999; Hoffman 2003, Paine et al. 2007
		Combining data	Smith et al. 1996; Tavani 1999
		Secondary use of data	Culnan and Armstrong 1999; Smith et al. 1996; Smith 1993; Stewart and Segars 2002; Hoffman et al. 1999a; 2003; Culnan 1993; Cranor et al. 1999; Rindfleisch 1997; Campbell 1997; Grupe 1995
		Selling data (Government)	Lopez 1994; Grupe 1995

- *Collection* – How much personally identifiable information is being collected and stored? What types of information are being collected?
- *Control* - How much control does an individual have over information in a business's database? Individuals would like to be able to explicitly give permission for businesses to use their information (i.e. opt-in).
- *Awareness of privacy practices*- How knowledgeable is the individual about privacy policies of a business?

A driving force behind these concerns is the fact that individuals want to feel in control of their personal information (Hine and Eve 1998, Hoffman et al. 1999a, 1999b, Hoffman 2003, Olivero and Lunt 2004), which is actually one factor that comprises the definition of privacy as identified above. If individuals do not feel in control, their privacy concerns are greater (Dinev and Hart 2003). For example, individuals do not like the idea of automatic data transfer, such as an auto fill button for a form (Cranor et al. 1999). An issue related to individuals' wishing to feel in control is that they would like to own their personal information (Mason 1986).

Research has investigated the importance of each of these concerns and their ranking. For example, one study found that individuals are most concerned about transfer (shared or sold to other parties), notice/awareness and storage (Earp and Anton 2004). Another found that improper access and secondary use are more important than possible errors (Hann et al. 2002a). Finally, there are actual levels of concern, which relate to specificity of information (Nowak and Phelps 1992).

1.3 Online Social Networking

The advent of online social networking has spurred new privacy related questions. Social networking websites are websites that allow users to congregate and share information with their friends and even strangers. They facilitate the building of communities of people with shared interests. Most social networking websites offer a variety of services to their subscribers including: blogging, video, chat, discussion groups, and messaging. Some of the popular social networking sites include: MySpace, Facebook, Friendster, and Orkut (Google). [For a history of social network sites see Boyd and Ellison (2007)]. Research on privacy on online social networks (OSN) is actually quite new. However, since, the actual premise of these websites is to share information there are clear privacy issues at stake. To illustrate, profiles can be used to real-world or online stalk since they often include information about class schedules and residence locations. In addition, similar to data-mining, using re-identification techniques, bits of information that are disclosed can be merged with other databases and recreated into more meaningful profiles (Gross and Acquisti 2005). Furthermore, users share information with friends, and since this information is digitalized, even if they don't intend to share personal information with strangers it can easily fall into the wrong hands. Last, users are sometimes not aware of the default settings on these websites, for example, on Facebook the default setting for a user's profile is used to allow anyone to view a user's entire profile, and even now a lot of information remains public if the privacy settings are not changed.

1.4 Research Question: Information Disclosure on OSN

When investigating these two streams of research (privacy and social networking) it is interesting to note that when it comes to disclosure on Online Social Networks, individuals don't seem to take their privacy concerns into account, and they will disclose a lot of private information *voluntarily* (see § 1.3 above). To illustrate, much research studies what individual's

concerns are, what they are most concerned about (i.e. Nowak and Phelps 1992, Phelps et al. 2000), and the various factors that affect and are affected by their concerns (i.e. Raab and Bennet 1998, Arami et al. 2004). These streams of research have identified numerous concerns (see § 1.2). Nevertheless, recent research on the use of OSN indicates that the information disclosure rate is enormous (Lenhart and Madden 2007, Barnes 2006). It seems as though when people use Online Social Networks, they do not consider their privacy values, and that their socialization becomes more important. Since it is crucial that personal, and especially personally identifying information, remain private, there is a need to examine this behavior in order to understand why this occurs.

Some research has examined privacy as a paradox, and has found that when it comes to privacy, people seem to be hypocritical with regard to their attitudes and actions (Norberg et al. 2007, Berendt et al. 2005, Connelly 2007, Acquisti and Grossklags 2004). There is an inconsistency in user behavior based on what they say their privacy concerns are, and more importantly, they state that their concerns are higher than their actual behavior reveals. To illustrate, Berendt et al. (2005) conducted an experiment to test just this and found that people reveal a lot of information to an online store, more than would be expected based on their privacy preferences. Similarly, Norberg et al. (2007), in an offline disclosure experiment, found that the amount of disclosed information exceeded the amount of information individuals *stated* they would disclose. Last, Connelly (2007) found that paper survey responses about privacy attitudes do not match disclosure behavior 'in-situ.' This 'paradox' can be better explained by examining the cognitive mediators identified by the Protection Motivation Theory.

This dissertation seeks to understand information disclosure and protection and to build a model examining this behavior specifically in the OSN environment. While privacy research may *partially* explain disclosure behavior this dissertation seeks to examine the cognitive processes involved in disclosure. Although it is understood that privacy is of the utmost importance, especially in today's increasingly open environment, this important piece of the disclosure process has not been addressed, and may ultimately shed light on the cognitive processes involved. More specifically, this dissertation seeks to examine: Can an all-inclusive comprehensive framework be built to explain privacy disclosure or non-disclosure in *all* situations, and more specifically in the OSN environment? What is the cognitive process with which individuals assess risk and threat in the Internet environment? What role do threat and efficacy play in disclosure? Does the type of interface affect comprehension of privacy settings?

1.4.1 Model

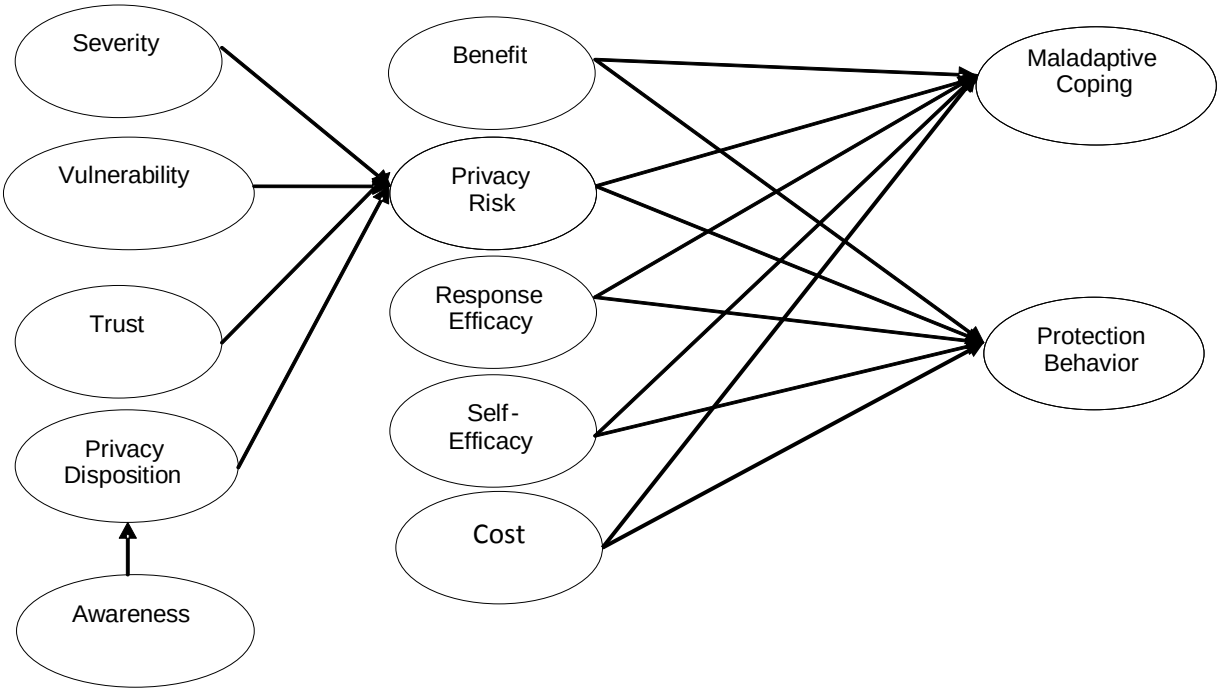
After reviewing the applicable literature, the following all-inclusive model has been proposed to explain disclosure behavior (see Figure 1 below). This model draws on both Social Exchange Theory and Protection Motivation Theory. The basic premise of Social Exchange Theory (SET) is, when people interact, either in real life or on the Internet, their actions are motivated by the expected returns, and this is the underlying concept guiding relationships (Blau 1964, Homans 1958). Social Exchange Theory is a sub-theory of Exchange Theory which explains that people choose from various alternatives so that they receive the greatest value at the lowest cost. (This idea draws from Economics' rational choice theory). There are many "flavors" of exchange theories, however, all have inherent in them the same fundamental concepts: exchange actors, exchange network, exchange resources, exchange structures, and exchange processes. As such,

an exchange involves the initiation - by an individual or groups in a network - of a trade for goods or services that is supported by the relationships between these actors and their subsequent interactions (Hall 2003). Exchange theory has been applied in research examining e-commerce, for example, to investigate developing protocols for fair exchange of digital products (Ray and Zhang 2007). In these types of exchanges individuals are interacting with a business with the purpose of purchasing a good or service. This exchange is mostly an economic one since there are specific guidelines that must be followed and precise contracts with terms and conditions that must be adhered to (Blau 1964).

A more common use of exchange theory in e-commerce is in the application of SET (sometime referred to as relational exchange theory). SET is often the principal underlying model used to explain which variables are important to be successful in an e-commerce venture, i.e. trust (Luo 2002). In this sense individuals may be persuaded to share their knowledge or information (i.e. name, address, credit card) to enter into a transaction in exchange for some resource. In fact, knowledge as a resource has been duly noted (Hall 2003). These basic principles remain the same when extending these theoretical ideas to exchanges that take place on social networking websites where information is exchanged for intangibles such as social approval and acceptance (Blau 1964).

A complementary theory that is examined is Roger's (1975, 1983) Protection Motivation Theory (PMT). The primary purpose of this theory is to examine how fear appeals affect attitudes and behavior. The objective is to examine and explain why people protect themselves from harm (or choose not to protect themselves) and how to ultimately persuade them to do so. PMT is mostly

Figure 1: Model of Information Disclosure



utilized in the context of preventive health in order to examine the effectiveness of different persuasion techniques to influence people to protect themselves from unnecessary risks [i.e. alcohol abuse (Stainback and Rogers 1983), smoking (Pechmann et al. 2003), and cancer risks (McMath and Prentice-Dunn 2005)]. Since its development, PMT has been applied in other contexts besides health including: marketing (Cismaru and Lavack 2006), environmental protection (Homburg and Stolberg 2006), crime (Cates et al. 2003), and in IS research (Youn 2005, Woon et al. 2005, Siponen et al. 2006). Thus, it is instrumental in understanding an individual's cognitive process and associated behavior when faced with *any* given threat (Rogers 1983) for which there is an "effective recommended response" (Floyd et al. 2000; p 409).

PMT is organized along two cognitive processes: threat and coping appraisal. In the threat appraisal process there are three main variables (rewards, severity, and vulnerability) which evaluate the maladaptive behavior (*not* following the recommended response to protect oneself, and to either not protect or to protect inadequately). In the coping appraisal process response efficacy, self efficacy, and costs evaluate the ability to effectively cope with and/or avoid the risk. To illustrate, in a threatening situation, an individual will evaluate:

a) the risks (severity and vulnerability),

b) the benefits (intrinsic and extrinsic rewards),

c) the ability to initiate the protective behavior (response efficacy),

d) the evaluation of the measures' effectiveness (self- efficacy),

e) the cost of taking the recommended action (response cost).

Therefore, in a threatening situation, these PMT variables are the cognitive mediators between a specific threat and the resulting coping method (behavior) (Rogers 1983) [(which can be either adaptive or maladaptive (Floyd et al. 2000, Rippetoe and Rogers 1987)]. The PMT variables are applied in this model as a way of opening the "black box" in order to examine in greater detail the cognitive processes an individual initiates when coping with privacy risk.

Research on information disclosure in the context of OSN is in its infancy. As such, building and testing a model (with both a survey and experiment), in order to explain protection and maladaptive behavior is an important first step in this new stream of literature. This proposed model is a synthesis of SET and PMT and also includes some interesting and important privacy-risk antecedents. The meshing of SET and PMT theories in this context should give a fresh perspective that will ultimately help explain disclosure behavior on OSN.

Chapter 2

REVIEW OF LITERATURE ON PRIVACY AND ONLINE SOCIAL NETWORKING

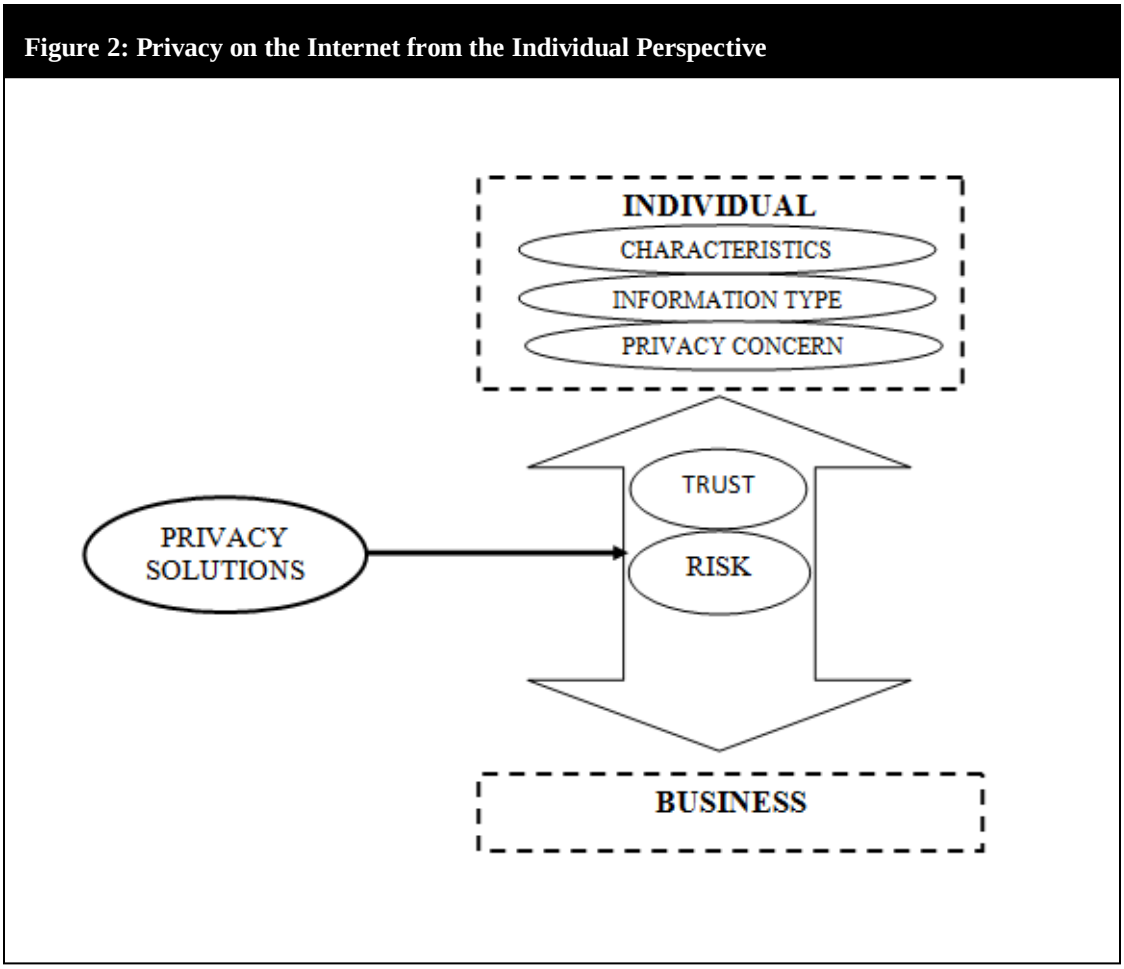
This section will review literature on privacy on the Internet in general, on OSN, and finally on privacy on social networking websites. Scholarly research on privacy on the Internet concentrates on identifying traits of individuals who are most concerned with privacy, and how privacy has an effect on behavior online. With regard to privacy on social networking, the little scholarly literature that is available concentrates on the reasons for using these websites, the types of information people reveal, and the surprising *amount* of information people reveal while using these websites.

2.1. Privacy on the Internet

When studying privacy, scholars investigate the various privacy issues from three different perspectives; government, individual, and business. They also study the interaction between the three perspectives (Boritz et al. 2006). The Government is the entity that provides the environment, regulation, and the context of the other two entities. There are many privacy issues between the government and individuals, as well as between the government and business. For example, with regard to the government relationship with individuals, research has studied why people should be concerned about government data collection, how privacy policies should apply to governments, and the attitudes of individuals towards government surveillance (Anderson and Dempsey 2003). With its relationship with businesses, the privacy issue focuses on the fact that the government has an enormous amount of sensitive data that is digital and must be protected when businesses connect with their databases (Joshi et al. 2002), for example, for e-procurement

(Hiller and Belanger 2001). However, these topics are beyond the scope of this paper. This dissertation solely investigates the Individual perspective. The framework depicted in Figure 2 can be helpful in categorizing what areas privacy research investigates and how the research areas are related.

Figure 2: Privacy on the Internet from the Individual Perspective



2.1.2 Privacy from the Individual Perspective

When studying privacy from the individual perspective, scholars examine three main issues: individual characteristics, type of information, and the many different types of concerns an individual may potentially have.

2.1.2.1 Characteristics

Privacy has always been an important matter. Some research focuses on the characteristics of people who want privacy. Current IS studies have extended previous research and have studied the many facets of the new privacy issues pertaining to the networked society, where information is more readily available and easier to access, and in particular the privacy issues related to the Internet. These various characteristics affect the degree of concern an individual may have. The types of characteristics can be divided into three categories: demographics, culture, individual traits, and experience.

Demographics:

Research has investigated how demographic information such as age, race, gender, geographical location, occupation, and education level effect privacy concerns (see Raab and Bennett (1998) for a summary on previous surveys). In general, variations of attitude of personal information use are accounted for by race, income, and education level (Raab and Bennet, 1998). In fact, gender, age, and education have also been studied as covariates to control for their effects on individual's reaction to privacy threats (Malhotra et al. 2004).

With respect to age, as age increases so do privacy concerns (Nowak and Phelps, 1992), and perceived risk of supplying personal information (Liebermann and Stashevsky 2002). In particular, older consumers are more concerned about data collection than any other privacy concern (Campbell 1997). Age is also associated with the likelihood of giving one's real name and attitude towards the importance of legal data protection (Arami et al. 2004). Gender has accounted for differences in privacy practices, attitudes and concerns as well. Research has found that men are less concerned about privacy than women (Kehoe and Pitkow 1999, Peslak

2006) and the latter provide more false information to protect their privacy (Kehoe and Pitkow 1999). In addition, females are less willing to disclose phone number, income and full name than males (Cazier 2002). There is also a relationship between gender and usage of protection software, gender and usage of anonymizing software, and gender and attitude toward the importance of legal protection (Arami et al. 2004).

Culture:

An additional factor that characterizes an individual who may have privacy concerns on the web is culture. Privacy concerns actually differ across cultures (Milberg et al. 1995, 2000, Davison et al. 2003, Bellman et al. 2004). For example, in the United States public opinion is mainly shaped by the media, which is largely controlled by big businesses, as opposed to Western European countries who value the protection of their personal information from businesses very highly (Davison et al. 2003). Research has also found differences in the way Americans and British perceive privacy and what their concerns are (Petrison and Wang, 1995).

Cultural values also play a role in explaining differences in levels of privacy concern. Research has found that high levels of certain cultural values such as individualism, masculinity, and power distance are associated with high levels of privacy concern (Milberg et al. 1995). Cultural values also affect the level of concern indirectly since they affect the amount of government involvement in protecting information privacy and, in turn, the regulatory structure of the government affects the level of concern (Milberg et al. 2000, Smith 2001). In other words, the different regulations mediate between the different values in culture and differences in privacy concern (Bellman et al. 2004).

Rights to privacy protection and privacy concerns may also differ across social groups and sectors. For example, non-white and less educated individuals claim to be less informed about name removal procedures than white and higher-educated individuals (Culnan 1995). Also, individuals from low-income families do not have any concerns regarding privacy on the Internet, (possibly because they do not have credit cards) (Jackson et al. 2003).

Individual Traits and Attitude:

Privacy concerns are also affected by individuals' traits such as being an extrovert/introvert, their value compatibility, and materialism. For example, consumers who are extroverts tend to disclose information when social adjustment benefits (psychological benefit) are offered either through electronic or traditional media, and introverts tend to disclose information only through electronic media (Lu et al. 2004). Another important trait is value compatibility, which measures how compatible the values of the individual and the business are. This can have a positive or negative impact on information disclosure depending on how the values align (Cazier et al. 2002). Last, materialism (or an individual's "fixation with material goods") is a significant covariate increasing willingness to provide information (Ward et al. 2005, p. 26)

Attitude is also a factor that affects privacy concerns. For example, an individual's attitude toward secondary information use impacts his concerns about privacy and control over personal information (Culnan 1993). In addition, people may adjust their privacy attitudes depending on their perceptions of the amount of privacy they can realistically acquire (Petrison and Wang, 1995).

Experience:
Research also investigates how the amount of experience an individual has with the Internet plays a role in the magnitude of his privacy concerns. Some research has found that the more proficient users were in using the web, the greater their privacy concerns were (Hoffman et al. 1999a; Miyazaki and Fernendez, 2001, Liebermann and Stashevsky 2002, Malhotra et al. 2004, Kuhlmeier and Knight 2005). Other research has found the opposite: the more experienced a user is the less concerned he is about privacy (Bellman et al. 2004). These conflicting results may be explained by the fact that more experienced users are more aware of what circumstances warrant concern, while novices do not understand the types of information that need protection and how websites can collect information and legally transfer it to a third party. They also do not understand the limitations and advantages of personalization (Earp and Anton, 2004). So, more experienced users understand that information may be collected over the Internet, which does warrant concern. However, they understand the types of information to protect and how to protect themselves.

2.1.2.2 Information Type

Privacy is highly valued by the consumers who expect the information they share to be private. As noted above, huge amounts of information are collected electronically and digitized which leads to concerns regarding disclosure. Researchers have focused on the types of information typically collected on the Internet, and Table 2: Information considered private, provides a list of information individuals are concerned about disclosing.

Table 2: Information considered private	
Information	**Reference**
Age	Culnan, 2000; Phelps et al. 2000
Address	McGinity, 2000; Cranor et al. 1999; Gindin, 1997; Culnan, 2000
Credit card numbers	Hoffman et al. 1998; Cranor et al. 1999; Gindin, 1997; de George, 1999; Culnan, 2000; Nowak and Phelps, 1992
Contents of the consumers' data storage device	Hoffman et al. 1999b
Date of birth	McGinity, 2000; Nowak and Phelps, 1992; Culnan, 2000
Demographic information	Culnan, 1999; Cranor et al. 1999
Education	Culnan, 2000; Phelps et al. 2000
E-mail	Cranor et al. 1999; Tu, 2002; Meeks, 1999; Oliver, 2002; Spior and Ward, 1995; Weisband and Reinig, 1995; Kirsh et al. 1996; Gindin, 1997; Panepinto, 1995; Culnan, 2000
Health care information and medical records	O'Brien and Yasnoff, 1999; Grover et al. 1998; Cranor et al. 1999; Gindin, 1997; Glenn, 2000; Kelly and Unsal, 2002; Nowak and Phelps, 1992
Income	Nowak and Phelps, 1992; Phelps et al. 2000
Name	Cranor et al. 1999; Gindin, 1997
Occupation	Culnan, 2000; Phelps et al. 2000
Phone number	McGinity, 2000; Cranor et al. 1999; Culnan, 2000, Nowak and Phelps, 1992
Purchase Behavior	Nowak and Phelps, 1992; Phelps et al. 2000
Real time discussion	Tu, 2002
Social security number	McGinity 2000; Berghel, 2000; Cranor et al. 1999; Gindin, 1997; Rotenberg, 1994; Culnan, 2000; Nowak and Phelps, 1992
Usage tracking/click streams (cookies)	Cranor et al. 1999 ; Aljifri and Navarro, 2004; Wang et al. 1998; Hoffman et al. 1999b; Grover et al. 1998; Hoffman, 2003; Fox, 2000; Resnick and Montania, 2003; Hale, 2001; Gindin, 1997; Miyazaki and Fernandez 2001

While examining the many different types of information collected, it is important to note that the *quality* of information is very important since "not all personal information is equal" (Berghel, 2000). Scholars differentiate between information types and agree that there are certain types of information that are more sensitive. However, sensitivity varies by context and individual (Sheehan and Hoy 2000, Malhotra et al. 2004). In general, sensitivity can be defined as the ability for information to be linked to other personal information (Wacks 1989). As such, it is often synonymous with personally identifiable information (Sheehan and Hoy 2000, Phelps et al. 2001). Thus, it becomes clear why people are more concerned about releasing their social security number than their favorite color.

Research has attempted to categorize information by how identifiable it is. The more identifiable the more concerned, and sensitive people are about disclosing it. The Federal Trade Commission (FTC, 2000) has classified information into three broad, high-level, and all-inclusive groups: personally identifiable, non-personally identifiable and anonymous. Personally identifiable information is information that is unique such as social security number, whereas, non-personally identifiable information is not identifiable unless it is combined with other information (i.e. first name). Last, information may also be anonymous (FTC, 2000). (Note that non-personally identifiable information, when alone and not combined with other information is the same as anonymous). Research has looked more closely at the different types of information people disclose and arranged them into levels that range from most likely to disclose to least likely. These categories are: demographic, lifestyle, purchase related, personally identifiable, and financial (Phelps et al. 2000). Many scholars use this classification as their basis and draw on

these categories to design disclosure experiments that manipulate information sensitivity (Malhotra et al. 2004, Sheehan and Hoy 2000).

Table 3: Framework for information types (based on FTC 2000, Phelps et al. 2000)

	Personally Identifiable	***Non-personally Identifiable/ Anonymous***
Demographic	Address Name Social security number	Age Education Date of birth
Lifestyle		Click streams Usage Tracking Cookies Contents of data storage device Real time discussion Hobbies Magazines Leisure activities
Purchase-Related		Purchase behavior Cookies Web-logs Most recent purchases
Financial	Credit card number	Income Level

To come up with a synthesized framework to arrange the many types of information by the sensitivity, the FTC (2000) and Phelps et al. (2000) categories can be arranged on opposing axes as depicted above in Table 3: Framework for information types (based on FTC 2000, Phelps et al. 2000). The Personally Identifiable category from Phelps et al. (2000) is not used since it is redundant. The Phelps et al. (2000) categories, and the information types from Table 3: Framework for information types (based on FTC 2000, Phelps et al. 2000) is mapped into the appropriate cells. Since it has been noted that sensitivity will vary by context and individual (Sheehan and Hoy 2000, Malhotra et al. 2004) the order within each cell is not significant.

2.2 Perceived Privacy Risk

Perceived risk has been studied in a variety of contexts such as: pharmacist behavior (Carroll et al. 1986), technology adoption (Featherman and Pavlou 2003, Yiu et al. 2007), health (Ma et al. 2007, Rindfleisch and Crockett 1999), and portfolio management and investments (Cho and Lee 2006, Forlani and Mullins 2000). It has also been an important variable in the marketing and consumer behavior literature since its introduction by Bauer (1967) as "consequences which he [consumer] cannot anticipate with anything approximating certainty, and some of which are likely to be unpleasant" (p24). Perceived risk has been defined as the "subjective expectation of loss" (Taylor 1974), or the "possibility of loss" (Yates and Stone 1992, p 4). However, other scholars have defined risk as being made up of two components that vary according to the researcher. Mitchell (1999) conducts a comprehensive review of all the various definitions and conceptualizations. He comes to the conclusion that although a universal definition has not been agreed upon, most empirical research has used Cunningham's (1967) model with success. As such, risk is conceptualized as being made up of the following two elements: consequences and uncertainty. These are defined as the importance of negative/unfavorable consequence and the probability of these negative consequence occurring. Save for the debate on what the two components of risk are, there also seems to be differences of opinion on whether to use these two components in an additive or multiplicative model (Mitchell 1999). Nevertheless, the two components can be considered as two facets of perceived risk (Cases 2002).

When conducting an online transaction there are a series of unknowns which can increase the perception of risk since the transactions do not take place face-to face (Kollock 1999). Seven dimensions of risk have been identified [see Table 4: Dimensions of Risk (based on Roselius 1971, Jacoby and Kaplan 1972, Peter and Tarpey 1975)]. Recently another facet of risk has been

acknowledge, privacy risk. It is defined as the probability that personal information will be disclosed, and research has found that individuals actually find privacy risk more important than any other type of risk (Cases 2002).

Table 4: Dimensions of Risk (based on Roselius 1971, Jacoby and Kaplan 1972, Peter and Tarpey 1975)

Type of risk	**Definition**
Financial	Monetary loss
Time/Convenience	Waste time researching the product and potentially make a bad decision
Psychological	Negative effect on the person's self-perception, loss of self-esteem
Social	Loss of status in social group
Performance	Item fail to meet performance expectations
Physical	Bodily harm
Overall	Likelihood of general dissatisfaction

Research concerning perceived risk has studied both the antecedents and consequences. With regard to the antecedents, research has found that familiarity (Van Slyke et al. 2006), less sensitive information (Malhotra et al. 2004), reputation (Chen and Dubinsky 2003, Tan 1999), site recommendation (Garbarino and Strahilevitz 2004), individual's privacy concern (Van Slyke et al. 2006, Malhotra et al. 2004), brand image (Tan 1999) and past Internet experience (Liebermann and Stashevsky 2002, Kuhlmeier and Knight 2005) all reduce perceived risk. In addition, demographic variables such as culture (Choi and Geistfeld 2004, Kuhlmeier and Knight 2005), age (Ueltschy 2004, Liebermann and Stashevsky 2002), gender (Ueltschy 2004, Garbarino and Strahilevitz 2004), and marital status (Liebermann and Stashevsky 2002) also have an effect on the perception of risk.

2.3 Trust and Privacy

Trust is related to risk and to privacy. Researchers have found that it alleviates concerns relating to information abuse, and eases cooperation among people (Friedman et al. 2000, Dinev and Hart

2002). Trust can be defined as, "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (Mayer et al. 1995, p 712). When conducting an online transaction, trust is even more important since the exchange does not take place face-to-face (Reichheld and Schefter 2000).

Risk and trust are very closely related. Literature investigating their relationship has not reached a consensus on which variable is the antecedent. Mayer et al. (1995) explain this relationship in more detail. They clarify the difference between "'willingness' to assume risk and actually 'assuming' risk…. [where] Trust will lead to risk taking in a relationship, and the form of the risk taking depends on the situation" (p. 724). In this sense the amount of trust one party has in the other party in a relationship, will determine the amount of risk the former party will take in a specific context (perceived risk). Research in e-commerce has found that trust increases purchase intentions directly (Gefen 2000, Van Slyke et al. 2006, Malhotra et al. 2004) and through perceived risk (Jarvenpaa and Tractinsky 1999 , Morgan and Hunt 1994, Kimery and McCord 2002, Ganesan 1994, Jarvenpaa et al. 2000, Van Slyke et al. 2006, Malhotra et al. 2004).

When investigating privacy risk in particular, research has shown that trust and control relate to customers' disclosure tendencies, and trust can suppress their privacy concerns (Hoffman et al. 1999b, Xu et al. 2003, Olivero and Lunt 2004) as well as reduce risk and uncertainty which ultimately leads to increased willingness to disclose information (Rohm and Milne 2004, Van

Slyke et al. 2006, Pavlou et al. 2005, 2007). Perceived risk actually mediates this relationship (Pavlou 2003, Jarvenpaa et al. 2000, Kollock 1999).

2.4 Protecting Privacy and Reducing Risk

Previous sections have discussed the many privacy issues that are at stake, and while no solution is perfect (Culnan and Bies, 2003), some research has investigated possible resolutions. Most fall into three categories: self-regulatory, government regulation, and technological innovation. All of the solutions aim to reduce risk and increase trust by using one or both of the risk reducing strategies identified by Cox (1967):

1. "Reduce the amount at stake"
2. "Increase feeling of certainty that loss would not occur." (p. 38)

The proposed resolutions are beyond the scope of this paper.

2.5 Online Social Networks and Privacy

Since people use the Internet as a social extension of themselves, investigating the privacy issues it creates is extremely important. When people use pseudonyms or fantasy characters to portray themselves on OSN the risk is not too great. However, when people use a digital social environment (i.e. social networking website, instant messaging, blogging) to supplement their day to day interactions a breach in privacy can effects the person's real life reputation (Nabeth 2005). Therefore, it becomes apparent that studying users' disclosure habits is very important.

The concept and theory of social networks, was first studied by Barnes (1954) and subsequently has been investigated extensively (for a literature review see Hatala 2006). In general a social

network can be defined as a community of people and the relationships between them. OSN differ slightly, primarily because relationships are visible (Boyd and Ellison 2007), the networks are much larger, and they have more weak ties (Gross and Acquisti 2005). In addition, they possess the same disadvantages as any other type of computer mediated communication, lack of nonverbal cues (Brown et al. 2007). Since OSN are a recent phenomenon research is only beginning to explore the many facets.

Research on OSN can be divided into four categories: impression management and friendship performance, networks and network structure, online/offline connections, and privacy issues (Boyd and Ellison 2007). The category investigated in this dissertation is privacy issues, all others are beyond the scope of this dissertation. Since research in this area is still quite new, to date there are few studies of research on privacy in social networks and these studies focus mainly on the safety issues for teenagers (Barnes 2006, Stuzman 2006, Lenhart and Madden 2007), the surprisingly vast amount of private information that people disclose (sometimes contrary to their privacy attitudes) (Acquisti and Gross 2006, Gross and Acquisti 2005, Jones and Soltren 2005, Lenhart and Madden 2007, Barnes 2006), and their willingness to share information (Dwyer et al. 2007). The findings of the above research can be grouped into two main categories: identification of types of information disclosed and identification of motivation for disclosure.

Survey research has shown that OSN users tend to share many types of information including (for college students) very personal information such as, birthday (84%), cellphone number (34%), home phone number (10%), personal address (24%), schedule of classes (42%), political

orientation (53%), instant messaging name (75%),sexual orientation (59%), and partner's name (28%) (Acquisti and Gross 2006). Teenagers (which make up much of the user base of OSN) tend to disclose information such as: first name (82%), photo (79%), photo of friends (66%), city or town (61%), school (49%), instant message screen name (41%), e-mail address (29%), and last name (29%) (Lenhart and Madden 2007).

With regard to motivations, research has found, that students become members of social networking websites for two main reasons: a) friend recommendation and peer pressure, or b) as an extension of their socialization to meet new people, make new friends, find old friends, and keep in touch (Govani and Pashley 2006). More recent research has identified seven categories of uses for Facebook (Joinson 2008), these are: Shared identities, Social connection, Photographs, Content, Social investigation, Social network surfing, and Status updates.

This review of privacy and OSN literature identifies a gap in explaining disclosure on OSN, and in identifying the cognitive processes involved in making the decision to protect private information. Therefore, the following section draws on theory and previous research to examine the relationships proposed by the model in § 1.4.1.

Chapter 3

THEORY AND HYPOTHESIS DEVELOPMENT

This section will review both Social Exchange Theory (SET) and Protection Motivation Theory (PMT), as well as, trust and risk theory, which are intrinsically intertwined with SET, to build a suitable background to develop hypotheses explaining disclosure and protection behavior on OSN. It will also explain in more detail each of the relationships described in the model above in § 1.4.1. This section is organized as follows: first, a broad description of SET and PMT and how they apply in this context is described; next, the hypotheses regarding the PMT cognitive processes are developed; finally, risk antecedents are discussed.

3.1 Social Exchange Theory

A social exchange is defined as the "voluntary actions of individuals that are motivated by the returns they are expected to bring" (Blau 1964; p91). In essence, social exchange is a basic building block of life, where people will do something (i.e. favor) based on the expected rewards. As such, SET is the basis of both long (Hall 2003) and short-term (Bignoux 2006) relationships since *all* exchanges can be conceptualized as social exchanges (i.e. giving charity) (Blau 1964). Social exchanges are different than economic exchanges. In a social exchange there are "*unspecified* obligations" (p8) where trust is essential, required and promoted, because there is no binding contract to enforce the terms of the exchange. So, when doing a favor, people expect the favor to be reciprocated, however, they cannot dictate exactly how, when, where, and the type of favor that should be reciprocated or fix a price for the favor. This is unlike a

calculated economic exchange where there is a contract with very specific details regarding compensation (Blau 1964).

In social exchanges, as with any exchange, cost and reward are two important factors, as, "human pleasures [rewards] have their root in social life (Blau 1964; p14)." These rewards [i.e. love, power, companionship] may have a cost that is not necessarily the same for every person, however, in general, "social situations are intrinsically rewarding" (Blau 1964; p15). In the privacy context the costs are privacy risks and concerns and the rewards are long term relationships either with a business as in e-commerce, or a social relationship as on a social network website.

Research in e-commerce has identified cost reduction techniques to benefit the businesses so that they can collect more information on their customers. For example, businesses try to reduce costs by alleviating privacy concerns. Trust is also a factor that can actually suppress privacy concerns, reducing the individual's cost, and thereby facilitating information disclosure (Xu et al. 2003). Consumers also prefer websites that provide notices of privacy protection, which also reduce costs (Hann et al. 2003). Rewards are positive reinforcement. SET states that individuals tend to perform actions that are rewarding. For example, within the privacy in e-commerce realm a reward may be a monetary reward or a convenience that may incite an individual to disclose personal information to an e-commerce business (Xu et al. 2003; Hann et al. 2003).

In a social situation, online or offline, a reward is more intangible; as such there are six types of rewards: social approval, social acceptance, respect, attraction, and power. Cost too is

intangible; it is time and effort (Blau 1964). On an OSN the reward is the same (as in an offline social situation) despite the fact that the *manner* of the exchange that takes place is different (not face-to-face).

To summarize, all exchanges can be conceptualized as social exchange, where people are motivated to do actions by evaluating the cost and rewards, which may be tangible or intangible (Blau 1964, Homans 1958). As such, sharing information online can appropriately be conceptualized as an exchange where the cost is privacy, time, and effort and the reward is one or more of the following: social approval, social acceptance, respect, attraction, and power. Hence, for a decision to be made regarding any disclosure benefits and risks must be weighed. Since SET states that individuals perform actions that are rewarding, in an OSN, if the benefits outweigh the risks (cost) individuals should be more likely to participate and disclose information.

3.2 Protection Motivation Theory

Protection motivation theory (PMT) is applied when examining human behavior and an individual's response to a given threat in any situation. The building blocks of this theory are the two cognitive processes of threat and coping appraisal (described in detail above in § 1.4.1). When individuals are faced with a threat there are six conditions that will lead them either to take actions to protect themselves, or to cope with the risk cognitively and to ignore the recommended protection mechanism. These conditions are the cognitive mediators: severity, vulnerability, benefit, cost, self efficacy, and response efficacy. These variables will ultimately influence the individuals' decision and initiate coping responses.

It is easier to consider the variables as part of a 2 x 2 matrix (see Table 5: Factors Effecting Response (PMT; Rogers 1975) below). All the variables will elicit either an adaptive (the recommended "good" response, i.e., to protect) or maladaptive (not following recommended response) response. Increasing rewards or decreasing the severity and vulnerability (risk) will increase the probability of a maladaptive response, and increasing response and self efficacy or decreasing costs of protection will increase the probability of an adaptive response.

Table 5: Factors Effecting Response (PMT; Rogers 1975)

	Increase	*Decrease*	
Maladaptive response	Intrinsic rewards Extrinsic rewards	Severity Vulnerability	**=Threat appraisal**
Adaptive response	Response efficacy Self efficacy	Response costs	**=Coping appraisal**

With these tools (the appraisals), an individual will take action to manage the resultant threat level with a coping mode that is either adaptive or maladaptive. Adaptive coping consists of initiating and/or continuing the recommended protective response and maladaptive coping is comprised of various cognitive coping strategies used while not taking the preventive action (i.e. hopelessness, avoidance, wishful thinking, and fatalism).

Protection Motivation Theory is appropriate to apply in the context of privacy on the Internet for a number of reasons. First, it has been noted that PMT can be appropriately applied in *any* situation where there is a threat and appropriate recommended response (Rogers 1983). Research investigating privacy on the Internet has found that privacy risk is a genuine concern of individuals (see § 1.2.1). In fact, a breach of Internet privacy can have far reaching effects in the real world (i.e. using information posted on Facebook to stalk), and is ultimately a bodily threat just like a health threat is. Last, it has been successfully applied in IS context (i.e. Youn 2005,

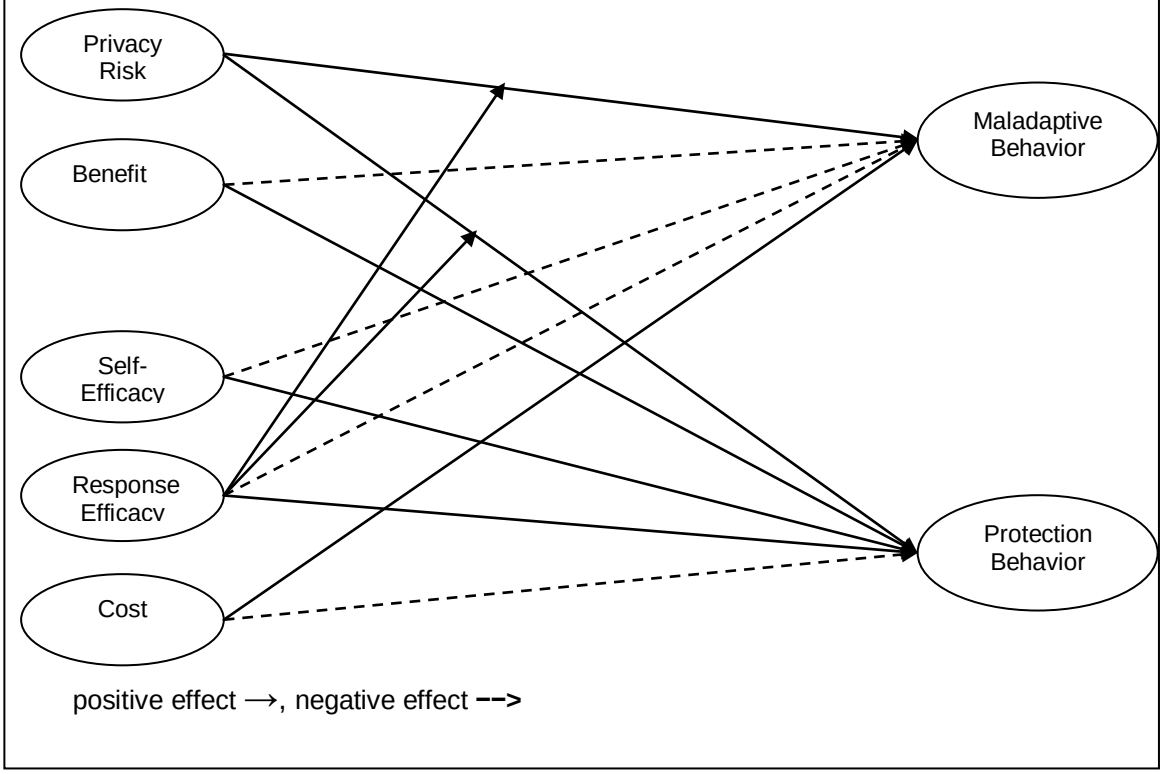
Woon et al. 2005, Siponen et al. 2006, Chenoweth et al. 2009, Workman et al. 2008). For example, LaRose and Rifon (2007) apply PMT in the privacy realm in exactly the same manner it is studied in health. They analyze how to encourage individuals to protect themselves on the Internet. Other studies (i.e.Chenoweth et al. 2009, Siponen et al. 2006) study compliance with IS security measures. Most noteworthy is Workman et al.'s (2008) study that investigates individuals' attempts to circumvent security measures deliberately. Their study draws on PMT, but fails to incorporate maladaptive behavior which is an important predictor of behavior in PMT research.

In the context of this study it is applied as follows: when an individual interacts with the Internet and OSN there are inherent risks and concerns associated (i.e. privacy), of which people usually are aware. This has been well established in the literature. However, although people are aware of the associated risks, often they choose to ignore them and to disclose information despite the consequences. Research on privacy has observed that on OSN this phenomenon is usually exacerbated, where people seem to be disclosing many different types of information without properly assessing the consequences (see § 2.5). This behavior can be explained by examining the protection motivation process. To illustrate the parallels; many PMT studies seek to examine threats and why individuals do/do not adopt recommended treatments. For example, (Greening 1997) examines teens smoking behavior using PMT and finds that the cognitive variables adequately explain smoking and non-smoking behavior. Similarly, examining the PMT variables in the privacy risk context should adequately explain why individuals do/do not adequately protect themselves when disclosing information on social networking websites.

3.3 PMT Cognitive Process Variables

As discussed above, there are two major cognitive processes involved in the decision of whether or not to disclose information. These are the threat and coping appraisals that the PMT describes. These two processes work together to determine intentions, as well as, behavior (Milne et al. 2000). The effect of the PMT cognitive process variables is indicated in Figure 3: Relationship between cognitive process variables and coping modes below.

Figure 3: Relationship between cognitive process variables and coping modes



3.3.1 Threat Appraisal

The threat appraisal evaluates the consequences of not taking recommended protection precautions by weighing the severity (seriousness) and vulnerability (probability of occurrence) of the threat, as well as benefit, or rewards, associated with not initiating a protective response.

In an OSN setting, the associated risk is privacy risk (i.e. identity theft). The benefits/rewards are intangible, such as communication, and social investigation (Joinson 2008).

3.3.1.1 Risk

Both SET and PMT identify risk as an important component. As SET indicates, costs and rewards are an integral part of any exchange. In PMT, risk is a component of the threat appraisal which impacts the type of coping that will be initiated. Although risk is not obviously denoted in the original PMT model, severity and vulnerability are in fact the two components that make up risk (Mitchell 1999).

Risk simply put, is the probability and magnitude of loss or gain (Douglas 1992). Risk is sometimes treated as objective or subjective (Mitchell 1999), but for this research it will be treated as a subjective measure, as such it is inherently socially constructed. It is a concept people use to "help them understand and cope with dangers and uncertainties of life." (Slovic 1999; p 690). When individuals are confronted with situations that have uncertain consequences that may cause discomfort, they will evaluate the likelihood of these consequences, their own personal acceptable level of risk, and the significance of the risk or benefit, and only then will they take an appropriate action (Dowling and Staelin 1994, Youn 2005, Cho 2004).

Perceived risk has been studied in many different areas including psychology, sociology, and marketing. Research has agreed that there are many components of risk including: inherent risk, handled risk, accepted risk, and product specific risk (Bettman 1973, Dowling and Staelin 2003). In general, most definitions of risk agree that there are two main components: uncertainty and

consequences. Hence, perceived risk can be defined as the magnitude of unfavorable consequences and the probability that they will occur (Mitchell 1999). This is consistent with the many definitions of risk which propose that it is made up of two parts: severity (magnitude) and vulnerability (probability). Perceptions of risk engender wariness of activities which can lead to risk handling behaviors such as purchasing from major brands, information seeking, reducing the amount at stake (Roselius 1971, Dowling and Staelin 1994, Taylor 1994), and in the context of online behavior removing information online, providing inaccurate information, or not doing business with online firms (Milne et al. 2004, Youn 2005).

Research has identified seven sources of the perception of risk (see Table 4: Dimensions of Risk (based on Roselius 1971, Jacoby and Kaplan 1972, Peter and Tarpey 1975) above). In general the Internet amplifies some risk dimensions (Tan 1999, Cases 2002). For example, time spent on making an online purchase, not receiving the product on time, credibility and reliability of web site, and invasion of privacy (Cases 2002). This dissertation concentrates on one particular aspect of risk: privacy risk, which is defined as the probability that personal information will be collected without the knowledge of the individual (Cases 2002). Therefore, applying the basic risk definition in this context, since severity and vulnerability are the two components of which risk is comprised, when the degree of harm of having personal information disclosed (severity) and/or the probability that this will in fact occur (vulnerability) increases, perception of privacy risk will increase.

Protection Motivation Theory states that individuals will protect themselves and prevent harm from occurring by weighing the risks and benefits. The outcome of this process is the coping

measures they take. Coping can take the form of adaptive and maladaptive strategies. Adaptive coping modes are forms of coping that actually deal with the threat and mitigate it by adopting the recommended protection mechanism, (i.e. using privacy settings). For example, Youn (2005) utilizes PMT to empirically validate the relationship between risk and reward, willingness to provide information, and the implementation of coping behaviors to protect privacy (i.e. providing incomplete or false information or leaving the site). As such it is expected that if the risks of providing personal information on OSN websites are perceived as high, individuals will engage in privacy protection behaviors.

Hypothesis 1: Perceived Privacy Risk is positively related to Protection Behavior

Maladaptive coping modes also provide a way for the individual to deal with perceived risk level by providing a method for the individual to cognitively deal with the emotions generated by the threat (by i.e. denying the existence of the threat (avoidance) or not accepting that this can happen (hopelessness)) (Rippetoe and Rogers 1987, Folkman and Lazarus 1980). PMT models treat coping differently. For example, Milne et al. (2000) in a meta-analysis use a model that treats maladaptive behavior as a predictor of protection motivation (which is measured as behavioral intention to protect), which in turn predicts actual behavior (protection); and Floyd et al. (2000) in a meta-analysis treat maladaptive behavior as a dependent variable that is the outcome of protection motivation. Additionally, Umeh (2004) notes that maladaptive behavior is sometimes measured as a mediator and sometimes as a moderator. Other research has studied maladaptive coping as the dependent variable (Rippetoe and Rogers 1975). Therefore, since the relationship between intentions, behavior, and maladaptive coping seems to be unclear. In this

research, maladaptive coping is used as a dependent variable. As such, when the risks are perceived as high, individuals will find a way to cognitively deal with the increased risk.

Hypothesis 2: Perceived Privacy Risk is positively related to Maladaptive Coping

3.3.1.2 Benefit

In privacy research, disclosure of private information is often described as a trade-off between the risk and reward. Privacy research has found a relationship between information disclosure and benefits. For example, on the Internet, there are four extrinsic benefits and three intrinsic benefits for which individuals will disclose information, these are: monetary savings, time savings, self-enhancement, social adjustment, pleasure, novelty, and altruism (Hui et al. 2006). The type of reward that will induce an individual to disclose information is specific to individual characteristics and is related to personality factors (Hui et al. 2006). Research has investigated particular situations and rewards and has found that individuals are willing to disclose private information in exchange for rewards such as, free membership to a club (Malhotra 2004), monetary rewards (Hann et al. 2002a, 2002b, Yang and Wang 2009), future convenience (Hann 2003b), preferred access to information (Norberg et al. 2007), and customized marketing offers (White 2004).

Reward is an integral part of both SET and of PMT. In SET the reward is the variable that induces an individual to enter into an exchange; this is weighed against the cost (Blau 1964). In PMT rewards are a part of the threat appraisal and they increase the probability of a maladaptive response (Rogers 1975). In a meta-analysis, Floyd et al. (2000) only found six studies that

included benefits in their models, however, the findings were all consistent with PMT propositions. Hence, the greater the reward, the more likely it is that the individual will not protect themselves and initiate maladaptive coping.

Hypothesis 3: Benefit is positively related to maladaptive behavior
Hypothesis 4: Benefit is negatively related to protection behavior

3.3.2 Coping Appraisal

The second cognitive process PMT describes is the coping appraisal. This process evaluates the individuals' ability to cope with the threat by assessing the perception that the individual can effectively perform the recommended behavior (self-efficacy), that the recommended behavior will actually be effective (response efficacy), and the associated costs of performing the recommended behavior.

3.3.2.1 Cost

Costs are the opposing factor to the rewards. Cost in PMT research refers to Response Costs, or the cost of initiating protective behavior (adaptive response). In each context response costs will be different. For example, in a health context, Prentice-Dunn et al. (2009) studied the use of sunscreen, and in this case response costs were measure as inconvenience of use of sunscreen and loss of benefit associated with a tan. In an information technology context, Liang and Xue (2009) measure it as time, money, and inconvenience to adopt an anti-threat system (i.e. anti-virus). In this context the cost refers to the time, effort, and inconvenience of setting up privacy settings on an OSN. This will be a factor that will have an effect on the initiation of maladaptive coping or protection behavior.

In both health related research and information security research, costs of adapting the recommended behavior will be weighed and if the cost is too high, the individual will not take the preventive measure (Prentice-Dunn et al. 2009, Woon et al. 2004, Liang and Xue, 2009, Chenoweth et al. 2009). As such, costs have been shown to be negatively related to protection intention and positively related to maladaptive coping. These effects have also been observed in two independent meta-analyses (Milne et al. 2000. Floyd et al. 2000).

Hypothesis 5: Cost is positively related to maladaptive behavior
Hypothesis 6: Cost is negatively related to protection behavior

3.3.2.2 Self efficacy and Response efficacy

Self efficacy in PMT research was originally modeled after Bandura's (1977) self efficacy and is defined as the perception that, "one can successfully execute the behavior required to produce the outcomes" (p. 193). Response efficacy is the perception of the effectiveness of the recommended response. These two components have been investigated a great deal in health related PMT research (i.e. Rippetoe and Rogers 1987, Fruin et al. 1992) and it has been found that they decrease the probability of a maladaptive response and increase the probability of the recommended response (Rogers 1975). This has been confirmed with two different meta-analyses: Milne et al. (2000) and Floyd et al. (2000). In IS survey research, self-efficacy and response-efficacy have been related to compliance to IS security policies (Siponen et al.2006, Johnston 2006, Herath and Rao 2009), adoption of anti-spyware software (Lee and Larsen 2009, Chenoweth et al. 2009) and avoidance of IT threats (Liang and Xue 2009). In this research protection behavior is measured. Thus, if in an individual believes that he has the ability to use

privacy settings, and that the privacy settings are effective in protecting their information, they will be more likely to disclose information since they have the perception that they can manage (cope with) the threat. They will also be more likely to use the privacy settings since they believe that they can and that the privacy settings are effective.

Hypothesis 7: Self efficacy is negatively related to maladaptive behavior
Hypothesis 8: Self efficacy is positively related to protection behavior
Hypothesis 9: Response efficacy is negatively related to maladaptive behavior
Hypothesis 10: Response efficacy is positively related to Protection Behavior

PMT research in the health realm has studied various interaction effects. In the original model Rogers (1975) predicted that perceived vulnerability, severity, and response efficacy would combine multiplicatively to influence intentions. He expected significant main effects for each variable, and two-way and three-way interaction effects among these three variables. However, few studies provided support for this model (Eagly & Chaiken, 1993). Many PMT studies have examined almost all possible interaction effects possible given the cognitive process variables, with mixed results. What intuitively makes the most sense are the interactions between threat and coping variables. For example, Sturges and Rogers (1996) find a significant interaction between threat and coping. Rippetoe and Rogers (1987) find a significant interaction between threat and efficacy; when there is high threat, low efficacy results in maladaptive behavior, and high efficacy results in protection behavior, this indicates that efficacy variables moderate the effect of threat on coping modes.

Witte (1992, 1994) extended PMT with the Extended Parallel Process Model which explains that threat must be high in order for there to be any response at all. When threat is high and response efficacy is low this will instigate maladaptive coping, since the individual does not feel that he had the tools to protect himself. Whereas, when threat is high and response efficacy is high, he will initiate protective behaviors. So, in this research the assumption is that privacy risk will have a direct effect on both coping modes, however, response efficacy will moderate this effect.

Hypothesis 11: Response efficacy and Perceived Privacy risk will have a positive interaction effect on Protection Behavior

Hypothesis 12: Response efficacy and Perceived Privacy risk will have a negative interaction effect on Maladaptive Behavior

3.4 Risk Antecedents

Pavlou (2003) uses the classification of Ring and Van de Ven (1994) who divide risks into either technology-driven (Environmental) or relational (Behavioral). He explains, on the Internet there is behavioral uncertainty because e-tailors can behave opportunistically which leads to economic risk (losing money), personal risk (unsafe product), seller performance risk (government does not adequately monitor the Internet), and privacy risk (losing private information). There is also environmental uncertainty since neither the consumer nor the e-tailer has full control of the Internet. This leads to economic risk and privacy risk (Pavlou 2003). With regard to social networking website, the same two categories apply. There is environment risk, which is linked to the fact that individuals do not have complete control over the Internet. There is also behavioral risk, which relates to the risk associated with whom the exchange is taking place with and subjective perceptions of risk. As such all antecedents to risk can be divided into either

environmental (related to the context and Internet/website) or behavioral (related to the individual characteristics) (see Table 6: Antecedents Classification).

Table 6: Antecedents Classification		
	BEHAVIORAL/ INDIVIDUAL	**ENVIRONMENTAL/ CONTEXTUAL**
RISK	Privacy Disposition Awareness	Trust in OSN Severity Vulnerability

There are many risk antecedents studied in privacy research, for example, culture (Choi and Geistfeld 2004), experience, age and gender (Doolin et al. 2005). However, in this research the variable chosen as risk antecedents are the ones believed to be the strongest predictors of risk in this context. To illustrate, with regard to risk and the individual factors, on an OSN there is no coercion to disclose information it is completely voluntary and every person's general privacy values are different. With regard to contextual factors, severity and vulnerability are both considered facets that will effect perceived risk, and trust can be measured particularly in an OSN context. Figure 4: Risk depicts the relationship between the risk antecedents and perceived privacy risk. These relationships are examined in more detail below.

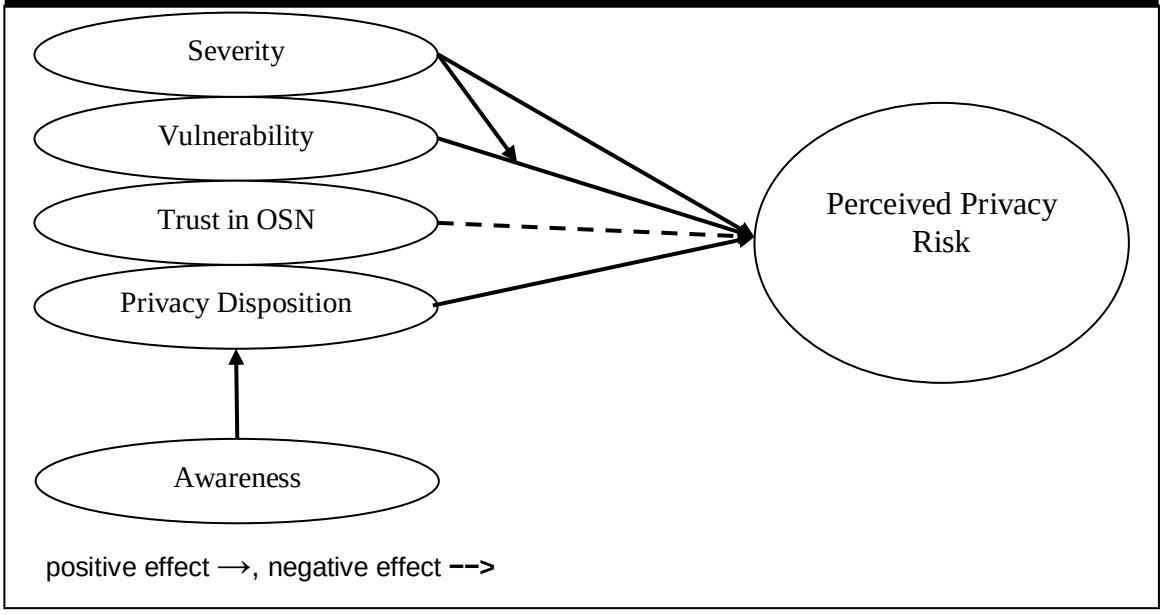
3.4.1 Privacy Disposition

Privacy research has studied the role of character traits that may affect perceptions in the privacy realm, one such trait is disposition to value privacy (Xu et al. 2009). Disposition to value privacy is the, "extent to which a person displays a willingness to preserve his or her private space or to disallow disclosure of personal information to others across a broad spectrum of situations and persons." (Xu et al. 2009). In this context it reflects a personal feeling of how much an individual feels that his privacy is important. Much research has delved into what

actually makes up privacy concerns. For example, both Smith et al. (1996) and Malhotra et al. (2004) came up with validated instruments to measure privacy concern. However, less research has actually looked into what the antecedents of privacy concern and privacy risk are. The amount of risk that an individual is willing to take will vary from person to person, since every individual has a personal threshold for risk tolerance (Das and Teng 2004), and the privacy concerns an individual has also varies from person to person (Xue et al. 2009). So, given the same set of circumstances, one person may feel concerned over the protection of his information and another may not be. Hence, the greater an individual's disposition to value his privacy the more privacy risk he will perceive.

Hypothesis 13: Privacy Disposition is positively related to Perceived Privacy Risk

Figure 4: Risk antecedents



3.4.2 Awareness

Awareness is defined as the knowledge or perception of privacy problems and consequences. This concept of awareness is different from the awareness that Malhotra et al. (2004) investigate as a part of their Internet Users' Information Privacy Concerns scale. Awareness in their case is defined as a measure of importance of transparency of privacy practices of companies. In this study awareness is similar to the technology awareness (TA) concept that Dinev and Hu (2007) develop based on Rogers (1995) innovation diffusion process. They explain that TA is an individuals' "raised consciousness of an interest in knowing about technological issues and strategies to deal with them" (Dinev and Hu 2007, p 391). In the context of OSN this is appropriate since knowledge of privacy challenges and/or protection strategies while using OSN is an important indicator of privacy disposition.

There aren't many studies analyzing awareness as a variable and how it affects privacy or other privacy risk variables. It is interesting to note that awareness programs are often recommended to increase knowledge of the privacy problem in order to initiate people into protecting themselves (i.e. Chellappa 2002, Acquisti 2004). Some research has touched on the awareness variable as part of a larger study and how it relates to disclosure practices and privacy concern. For example, there are many studies that investigate compliance of companies to the Fair Information Practices, of which one aspect is awareness, and how this affects consumers (i.e. Schwaig et al. 2006). Other research investigates disclosure. For example Milne and Rohm (2000) found that name removal preferences were affected by knowledge and awareness of name removal mechanisms (for direct mail, e-mail, and telephone), and Culnan (1995) found that consumers who are aware of name removal procedures have a lower privacy concern. Huang et al. (2004) found that awareness (knowledge) is a factor affecting perception of threat of

information security, and Olivero and Lunt (2004) found that subjects with more risk awareness want more control over their data. In a qualitative study, Andrews and Boyle (2008) found that communication sources (via mass media, marketers, and/or peers) help to shape risk perception online. The Electronic Privacy Information Center (EPIC 2006) explains that that many users are not aware of the privacy risks they take when interacting on OSN. However, awareness is an important predictor of disposition to value privacy, since the more in tune an individual is to the news, issues and consequences of various privacy matters, the more he will appreciate and value privacy (Xue et al. 2009).

Hypothesis 14: Awareness is positively related to Privacy Disposition

3.4.3 Trust

Trust can be defined as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (Mayer et al. 1995, p 712). This definition includes the two components important to every definition of trust across disciplines and levels of analysis: confident expectations, and willingness to be vulnerable (Rousseau 1998). These concepts are crucial in any relationship and social interaction. It is the basic belief that one party will not take advantage of the others' vulnerabilities and will behave ethically and consistently, which translates into a willingness to take a risk (Mayer et al. 1995).

There is a long established link between trust and risk which is grounded in exchange theory, commitment trust theory (which draws from exchange theory), and Luhmann's (1979) theory of

trust and power. Trust is necessary in a risky situation where the individual perceives negative consequences he has no control over (Koller 1988). If there is no risk and all variables of a situation are in the individual's control there is no need for trust (Luhmann 1979, Rousseau 1998, Scholsser et al. 2006). On the contrary, a very risky situation needs high levels of trust since there is a higher potential of deception (Kollock 1999), therefore, the degree of trust is a function of the degree of risk (Koller 1988). In addition, trust leads to risk taking in a relationship (Mayer et al. 1995) where the result of trust building is a reduction of perceived risk (Mitchell 1999). So, trust and risk have a circular relationship where "risk creates an opportunity for trust, which leads to risk taking" (Rousseau 1998, p 3).

The trust-risk relationship is an important one, especially on the Internet and when interacting with others on OSN since there is a great potential for loss (i.e. privacy, financial). Therefore, trust of the party that is being interacted must be addressed (Pavlou 2003, Belanger and Carter 2008). In e-commerce trust has been investigated as trust in the party (business) with which the transaction is occurring. Studies have found that trust reduces perceived risk in this context (Van Slyke et al. 2006, Malhotra et al. 2004, Kimery and McCord 2002, Pavlou 2003, Jarvenpaa 2000). Trust makes it possible for individuals to interact with a business and believe the business will behave ethically and with good intentions. Trust is an important aspect of Internet interactions (i.e. e-commerce), as the exchange does not take place face-to-face (Reichheld and Schefter 2000). It is more difficult to achieve online than in a traditional store since there is a lower cost of entry and exit to setting up an online store, and especially after the dot.com bust, it becomes obvious that these establishments are somewhat less stable than their traditional counterparts. It is needed so that the individual believes the online retailer will deliver the goods

and/or services as promised, their personal and financial information will not be compromised, and that one party will not take advantage of the others vulnerabilities in the transaction and act opportunistically (Jarvenpaa and Tractinsky 1999, Gefen and Straub 2004, Bhattacherjee 2004). While the use of the Internet exploded in the dot.com era as a business oriented medium, presently, the use of the Internet as a communications forum is taking becoming more and more prevalent. In this context instead of an economic exchange, there is a social exchange, and trust is important in this environment too. In fact, in a social exchange, trust is even more important than in an economic exchange since there is no binding contract (Blau 1964). Therefore, there is an inherent risk that the obligation or favor will not be returned (Molm et al. 2000, Blau 1964, Molm 2001). In this research and the context of disclosure on a social networking websites, there is an inherent risk associated with the OSN itself, which trust is expected to alleviate. Consequently, it is expected that trust will reduce the privacy risk perceived.

Hypothesis 15: Trust in OSN is negatively related to perceived privacy risk

3.4.4 Severity and Vulnerability

Both severity and vulnerability are components of risk. Severity can be defined as the perceived magnitude of the threat, and vulnerability can be defined as the perceived probability of the threat occurring. While all PMT research agrees that severity and vulnerability are both key parts of the threat appraisal process, (Rogers 1975, 1983), most research examines the direct effect of Severity and Vulnerability on the coping variables in both health and IT contexts (i.e. Rippetoe and Rogers 1987, Workman et al. 2008, Chenoweth et al. 2009, Prentice Dunn et al. 2009). However, the original model (Rogers 1975, 1983) actually incorporated fear arousal as a

variable that is effected by severity and vulnerability, and subsequently affects the coping responses, although not much research has been done on this mediating factor (i.e. Liang and Xue 2010, Arthur and Quester 2004, Meservy 2010).

In order to fully understand this mediating factor it is important to understand the difference between "threat" and "fear." Threat is defined as a risk or danger present in a situation whether or not the individual is cognizant of it, while fear is a cognitive reaction that is aroused when threat is perceived (Witte, 1996). In this research perceived threat is measured as perceived privacy risk, where perceived privacy risk is a specific type of threat – the threat of having private information misused. Therefore, both severity and vulnerability are antecedents of perceived privacy risk and they shape this variable. Meaning, both the magnitude of the potential threat to privacy and the probability that it will in fact occur will increase the perception of the risk of sharing information on an OSN. This relationship between severity, vulnerability and threat/risk is consistent with research in health and in online behavior. For example, Mesrvy and Banks (2010) find that severity and vulnerability both positively affect perceptions of threat, with regard to intention to use online social media. Liang and Xue (2010) find the same relationship in a technology adoption study. So, as an individual's perception of severity and vulnerability increases, their perception of risk will increase as well. In this context, as an individual's perception of severity of a privacy breach and their vulnerability to a privacy breach increases, their perceptions of the riskiness of sharing information online will also increase. Hence,

Hypothesis 16: Severity is positively related to Perceived Privacy Risk
Hypothesis 17: Vulnerability is positively related to Perceived Privacy Risk

The relationship between severity and vulnerability can actually be considered a moderated effect. In Rogers (1983) model it was proposed that there was a multiplicative effect. However, some research hypothesizes interaction effects, some do not, and the results are mixed. One reason for this may be that the interaction will only be significant in specific settings (Boer and Seydel, 1996). In health research, Pechmann et al. (2003) found significant interactions (with regard to protection motivation), but only in the extreme cases (very low or very high levels of the variables). Weinstein (2000) also found significant interactions in health research (with regard to protection motivation), but also only under specific conditions.

Based on the above health and IS research, it is expected that in the OSN context, the effect of vulnerability will be moderated by severity. That is, in order for an individual to perceive the threat, an individual must feel susceptible to the threat, since if the person does not feel vulnerable to the threat it does not make any difference how severe the threat is. However, the magnitude of this relationship between vulnerability and perceived privacy risk will be determined by the severity of the threat. As such, severity will moderate the effect of vulnerability since the extent of the maliciousness of the threat will not matter unless the individual feels susceptible in the first place.

Hypothesis 18: Vulnerability and Severity will have a positive interaction effect on Perceived Privacy Risk

Chapter 4

METHODOLOGY

Research in both privacy and in the OSN realm overwhelmingly employs survey research methodology. In this study, both a survey and two experiments will be conducted. The survey will test the main model in order to confirm the relationships between the variables in general. An experiment will also be conducted in order to triangulate these findings, by manipulating some of the more crucial constructs. A second experiment studies different interface types and how they affect comprehension of privacy settings.

4.1 Study1 - Survey

To empirically test the research model (see Figure 1 in §1.4.1), a survey was used for data collection. Data was collected in a large northeastern university in the United States from October-December 2010. Subjects were required to complete the survey as part of their course requirements, as such subjects self-selected. Data was collected from all OSN users, but for the analysis only data from the Facebook users was used since there were only 20 responses (.05%) from subjects who used an OSN other than Facebook. This context is appropriate since Facebook has over 250 million active users[2] , 54.5 million individual users each month, and is the fastest growing OSN.[3]

4.1.1 Data Analysis

SmartPLS 2.0 software (Ringel et al. 2005) was used to validate the measurement model and to test the hypotheses. Partial Least Squares (PLS) is a component based approach to modeling which tests the structural and measurement models in the same analysis. It analyzes the complex relationships between multiple independent and dependent variables simultaneously which results in a more rigorous analysis (Gefen 2000).

A total of 442 subjects were recruited, and after eliminating incomplete surveys, duplicates, and users who indicated that they used an OSN other than Facebook there were a total of 416 cases. This sample size is more than adequate based on two rules of thumb*: 1)* Chin and Newsted (1999) recommended ten times the maximum number of predictors based on the factor with the largest number of predictors, and *2)* Barclay et al. (1995) recommends ten times the number of

[2] http://www.facebook.com
[3] http://www.techcrunch.com/2009/01/13/social-networking-will-facebook-overtake-myspace-in-the-us-in-2009

items in the most complex construct (Gefen et al. 2000). For the 416 cases there were some random missing data points (.004 %). Mean replacement was used for this missing data since the complete case approach (using only cases that have all data) would result in an inappropriate sample size (Hair et al. 1998). In SmartPLS missing values are replaced by the mean of all items for the construct. When using PLS analysis, "there may be a small amount of data that are missing completely at random'' (Tenenhaus et al. 2005; p. 202).

Students are an appropriate sample for this research since adults between the ages 18-24 make up about 75% of all OSN users[4] and therefore their responses should be indicative of most users. In addition, 99% of individuals between the ages of 18-24 have an online social network account.[5] In this sample about 82% are between the ages of 18 – 25, which is consistent with the entire sample of Facebook users. This sample is split between males (44 percent) and females (55 percent). For all demographics see Table 7: Subject Demographics.

Table 7: Subject Demographics

Variable	Frequency (%)	Variable	Frequency (%)
AGE		**EDUCATION**	
18-25	339 (81.5%)	Freshman	5 (1.2%)
Over 26	70 (16.8%)	Sophomore	171 (41.1%)
Undisclosed	7 (1.7%)	Junior	204 (49%)
		Senior	22 (5.3%)
GENDER		BA	12 (2.9%)
Male	182 (43.7%)	Other	2 (0.5%)
Female	227 (54.6%)		
Undisclosed	7 (1.7%)		

Most constructs were measured using previously validated multi-item scales (see Appendix A) which were adapted to this context when necessary. The reliability of these scales in previous

[4] http://www.pewinternet.org/Reports/2009/Adults-and-Social-Network-Websites.aspx
[5] http://thepmn.org/pressreleases/060109?mp

research ranged from 0.71 to 0.92. When there was more than one scale available the scale that had greater reliability was used. Some items were added to the Perceived Privacy Risk scale in order to adjust the scale to this context. The awareness scale was based on Dinev and Hu (2007), but with changes in the wording to adapt to the OSN context. In particular, some items were adapted to pertain to privacy awareness in general and some to pertain to OSN privacy awareness. The benefits scale, cost scale, and protection behavior scale were all self developed, with care taken so that the resulting scale would be reflective.

Benefits measures the many intangible rewards obtained when using and OSN. In order to create this scale previous research on benefits and uses of OSN was examined (i.e. Pempek et al. 2009, Ellison et al. 2006, Joinson et al. 2008, Bumgarner 2007). Benefits or rewards are seldom measured in PMT research because they change for each context, as such, it is more difficult to create a scale since it is usually not possible to use existing scales. In addition, benefits are usually a multi-concept construct which usually makes the scale formative. Therefore, in order to use a reflective scale, the items used were the ones that depicted benefits that are related to communication with existing friends, which, based on research studying OSN use, is the most important aspect of OSN use (Ellison et al. 2006, Joinson et al. 2008, Govani and Pashley 2005). The cost scale was also self developed to measure the cost of using privacy settings (recommended response). As such, it was determined that the cost associated with using privacy settings would be time, effort, and inconvenience. This is consistent with the way cost is measured in PMT research (Liang and Xue, 2009a). Protection Behavior scale items were also self developed to measure change in the user's default privacy settings.

Table 8: Latent Variable Correlations

	AWARE	BENEFIT	COST	MAL	PB	DISP	RE	RISK	SE	SEV	TRUST	VUL
AWARE	**0.77**											
BENEFIT	0.06	**0.82**										
COST	0.06	-0.10	**0.84**									
MAL	0.04	-0.11	0.28	**0.82**								
PB	0.19	0.25	-0.34	-0.14	**0.78**							
DISP	0.47	0.01	-0.04	0.04	0.22	**0.81**						
RE	0.11	0.20	-0.11	-0.31	0.28	0.03	**0.85**					
RISK	0.20	-0.04	0.04	0.38	0.14	0.37	-0.17	**0.75**				
SE	0.15	0.28	-0.25	-0.34	0.42	0.06	0.55	-0.08	**0.80**			
SEV	0.18	-0.01	0.23	0.33	-0.02	0.27	-0.06	0.56	-0.20	**0.83**		
TRUST	0.06	0.03	0.18	-0.10	-0.11	-0.22	0.28	-0.32	0.11	-0.05	**0.87**	
VUL	0.12	-0.01	0.04	0.41	0.03	0.28	-0.25	0.65	-0.13	0.47	-0.32	**0.78**

NOTE: Self correlation was replaced with the square root of the AVE
AWARE=awareness; MAL=maladaptive behavior; PB=protection behavior; DISP=privacy disposition; RE=response efficacy; SE=self efficacy; SEV=severity; VUL=vulnerability

4.1.2 Measurement Validation

Discriminant and convergent validity were both evaluated. First, the item loadings were examined to assure that the items load higher on their construct than on any other construct and that there were no cross loadings. See appendix B for cross loadings. After examining the loadings a few items were dropped which has extremely low loadings[6]. The remaining loadings are all >.7 (Thompson et al. 1995). COST1 is .68, which is marginally lower than .7, but the item was maintained so that the scale would have at least 3 items. All loadings are significant at the $p<.01$ level for both Pearson and Spearman's correlations. This was accomplished by using the procedure explained by Gefen et al. (2005) (see Appendix C). Discriminant validity can also be assessed using the Fornell and Larker (1981) method in which the square root of the average

[6] TRST3 had a loading of .64; RISK2 had a loading of .62 and RISK5 had a loading of .5

variance extracted (AVE) for each construct should be larger than its correlation with any other construct see Table 8: Latent Variable Correlations.

Table 9: Reliability

	Mean	S.D.	AVE	Composite Reliability	Cronbach's Alpha
AWARE	3.24	0.75	0.60	0.86	0.78
BENEFIT	4.09	0.59	0.67	0.89	0.84
COST	2.55	0.89	0.71	0.88	0.79
MAL	2.72	0.88	0.67	0.86	0.75
PB	3.88	0.72	0.61	0.83	0.68
DISP	3.61	0.74	0.65	0.85	0.73
RE	3.68	0.74	0.72	0.89	0.81
RISK	3.34	0.72	0.56	0.88	0.84
SE	3.97	0.60	0.64	0.88	0.81
SEV	2.93	0.90	0.69	0.87	0.78
TRUST	2.78	0.79	0.76	0.87	0.69
VUL	3.27	0.81	0.61	0.86	0.79

AWARE=awareness; MAL=maladaptive behavior; PB=protection behavior; DISP=privacy disposition; RISK=perceived privacy risk; RE=response efficacy; SE=self efficacy; SEV=severity; VUL=vulnerability

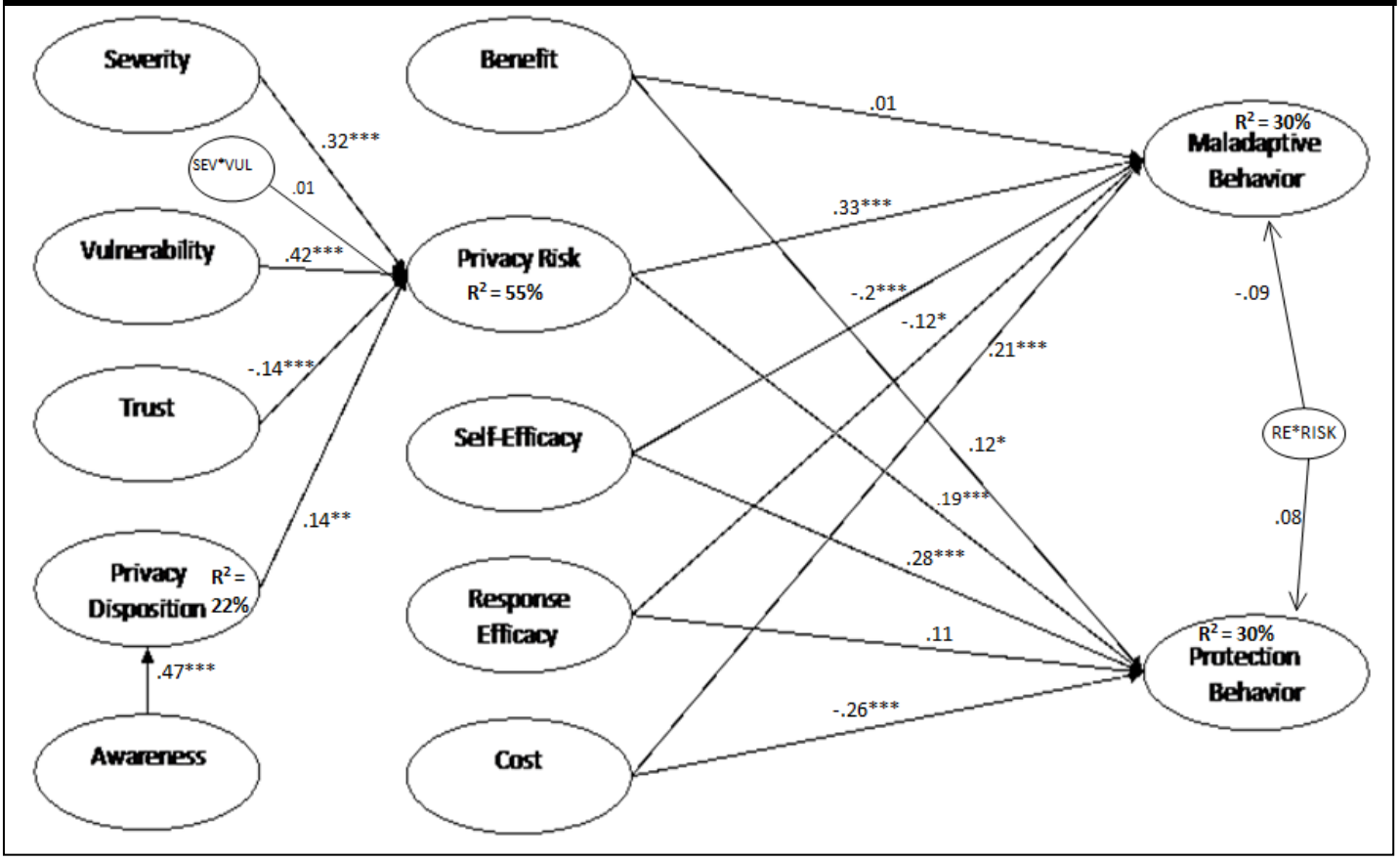
Reliability was assessed by examining Cronbach's Alpha for each construct, Dillon and Goldstein's Rho (Composite Reliability), and the Average Extracted Variance (AVE) scores. All constructs are reliable with Cronbach's Alpha >.7 (Nuanlly 1978), Dillon and Goldstein's Rho >.8, and AVE >.5 (Fornell and Larker 1981) which maintains measurement reliability, see Table 9: Reliability.

4.1.3 Measurement Model and Hypothesis Testing

This model accounts for 30% of variance towards Protection Behavior and 30% of variance towards Maladaptive Behavior. In addition, the risk antecedents account for 55% of the variance

towards perceived privacy risk and Awareness accounts for 22% of the variance in privacy disposition. See Figure 5: Model with path coefficients/beta weights for path coefficients.

Figure 5: Model with path coefficients/beta weights



For the risk antecedents, the effect of severity (β=.32, p<.001) and vulnerability (β=.42, p<.001) on perceived privacy risk is positive and significant. However, there is no significant interaction (β=.01), lending support for hypotheses H16 and H17, but not H18. Trust (β =-14, p<.001) has a significant negative relationship with perceived privacy risk, lending support for H15. Privacy disposition (β=.14, p<.001) has a significant positive relationship with perceived privacy risk, while awareness (β=.47, p<.001) has a significant positive relationship with privacy disposition lending support for H14.

For the cognitive mediating processes, there were two dependent variables; protection behavior and maladaptive behavior. For maladaptive behavior, perceived privacy risk (β=.33, p<.001) and cost (β=.21, p<.001) had significant positive relationships with maladaptive behavior, lending support for H2 and H5. Response efficacy (β=-.12, p<.05) and self efficacy (β=-.2, p<.001) had significant negative relationships with maladaptive behavior, lending support for H7 and H9. Benefit (β=.01) had a non-significant relationship with maladaptive behavior, therefore H3 is not supported. The interaction term for perceived privacy risk and response efficacy was not significant (β=-.09), therefore, H12 is not supported.

For protection behavior, perceived privacy risk (β=.19, p<.001) and self efficacy (β=.28, p<.001) and benefit (β=.12, p<.05) had significant positive relationships with protection behavior, lending support for H1, and H8, but H4 was not supported since a negative effect was expected. Cost (β=-.26, p<.001) had significant negative relationships with protection behavior, lending support for H6. Response efficacy (β=.11) had a non-significant relationship with protection behavior, therefore H10 is not supported. The interaction term for perceived privacy risk and response efficacy was not significant (β=.08), therefore, H11 is not supported (See Table 10 : Hypotheses for a summary of the results).

4.1.4 Discussion and Contributions

This study examined the role of the cognitive mediating factors of PMT, the role of benefits and costs from SET, and the antecedents of perceived privacy risk, and their combinatorial role in protection on an OSN. The results show that severity, vulnerability, trust and privacy disposition are all important factors that contribute to individuals' perception of privacy risk while using OSN. In addition, perceived privacy risk, benefit, self efficacy, and cost are all factors that

determine protection behavior, while perceived privacy risk, response efficacy, self efficacy and cost are factors that have an effect on maladaptive behavior. Interestingly, response efficacy was not a factor influencing protection behavior, and benefit was not a factor influencing maladaptive behavior.

Table 10 : Hypotheses		
H1	Perceived privacy risk is positively related to protection behavior	Supported
H2	Perceived privacy risk is positively related to maladaptive coping	Supported
H3	Benefit is positively related to maladaptive behavior	Not Supported
H4	Benefit is negatively related to protection behavior	Not Supported
H5	Cost is positively related to maladaptive behavior	Supported
H6	Cost is negatively related to protection behavior	Supported
H7	Self efficacy is negatively related to maladaptive behavior	Supported
H8	Self efficacy is positively related to protection behavior	Supported
H9	Response efficacy is negatively related to maladaptive behavior	Supported
H10	Response efficacy is positively related to protection behavior	Not Supported
H13	Privacy disposition is positively related to perceived privacy risk	Supported
H14	Awareness is positively related to privacy disposition	Supported
H15	Trust in OSN is negatively related to perceived privacy risk	Supported
H16	Severity is positively related to perceived privacy risk	Supported
H17	Vulnerability is positively related to perceived privacy risk	Supported
INTERACTION EFFECTS		
H11	Response efficacy and perceived privacy risk will have a positive interaction effect on protection behavior	Not Supported
H12	Response efficacy and perceived privacy risk will have a negative interaction effect on maladaptive behavior	Not Supported
H18	Vulnerability and severity will have a positive interaction effect on perceived privacy risk	Not Supported

The results of this study make important contributions to PMT, SET, and privacy risk research. First, the PMT model has been successfully implemented in a privacy risk setting and therefore extended its use in this context. The relationship between risk, cost, and self-efficacy with the dependent variables of protection behavior and maladaptive behavior were as expected. However, there wasn't a significant relationship between response efficacy and protection behavior. Previous PMT research has examined the role response efficacy has in predicting intentions (as a proxy for behavior) and finds a significant relationship. The non-significant

relationship suggests, that in this context (since this study only measures behavior) perhaps intentions do not predict behavior. Another plausible explanation is the measurement of protection behavior used in this study. In an OSN setting, there are many ways an individual can protect his privacy. For example, he can choose not to disclose information, he can remain anonymous, he can use a false identity, or he can disclose some information and not other. In the scale used in this study, only one aspect of protection was chosen: changing the default settings in the OSN account. As such, it is possible that had a formative measure of protection behavior been used, or measured a different aspect, the results may have been different. One last possibility is on an OSN the effectiveness of privacy settings is not an important factor that users take into account when using OSN.

The role of benefit was also surprising. Benefit had a significant *positive* relationship with protection behavior, and did not have a significant relationship with maladaptive behavior. The insignificant relationship was unanticipated because one of the main stays of PMT is the role that rewards have on individuals initiating maladaptive coping. According to PMT research, the more benefit perceived, the more likely the individual will NOT protect themselves. So in this case the more benefit (in terms of communication with friends) the *less* likely that individuals will protect themselves. However, the results of this research indicate that when using an OSN, the more benefits perceived (in terms of communication with friends, etc…) the *more* likely it is that an individual will protect himself. One possible reason for this is because benefits was measured as only having one dimension: communication with friends. However, it can be argued that benefits is a multi-faceted construct. In addition, when investigating this relationship further a model was analyzed that included a measure of disclosure of information to friends

only. This was an imperfect measure which is why it wasn't included in the full model, but it is interesting to note that benefit had a highly significant relationship with disclosure (to friends only). This serves to possibly explain the insignificant and counterintuitive relationships with the dependent variables. It suggests that benefits are taken into account when disclosing information and that these benefits apply strictly to disclosure to friends only. This seems to imply that people *do* disclose information *to their friends* (which means they do protect themselves somewhat by not disclosing their information to everyone, and hence have changed their default settings). This also serves to demonstrate the value people put in their personal conversations and the fact that some thought goes into disclosure. Last, it indicates that more research is needed particularly with regard to this variable and its role in OSN disclosure and protection.

All the hypotheses with regard to interaction effects were not significant. In general research in PMT has had mixed results when studying interaction effects. Some of these mixed results are the result of the two possible ways of studying the PMT model (additive or multiplicative). However, in this case the insignificant result is most likely due to the difficulty of modeling interactions with partial least squares. In fact, many studies have been examining the correct way to model such interactions. For example, Chin et al. (1996) explain that based on the work by Aiken and West (1991), the power to detect an interaction is decreased by up to one half if the readabilities of the constructs are .8 as opposed to 1.00, and up to two-thirds if the reliabilities are .7. In Smart PLS interactions are modeled based on Chin's (2003) recommendations which take the product indicator approach and after centering the indicator, multiplies each indicator in construct A by each indicator in construct B (i.e. *a1*b1, a1*b2*…). Goodhue et al. (2007)

conducted a comprehensive study of Chin's (1996, 2003) data, and found that although using the product indictor resulted in higher path coefficients, the statistical power (compared to regression) is much lower. This results in a lower probability of obtaining a significant interaction in the first place.

This research has shown that, with regard to OSN, perhaps benefit is not as important as cost in the trade-off. Meaning if the cost of losing control of information is too great, regardless of the benefit people will protect themselves. This research has also re-confirmed the role of privacy risk antecedents in privacy risk research and the role of trust as an antecedent and extended their use to OSN. The use of severity and vulnerability as antecedents to risk in the PMT model is also unusual. Few studies have measured threat or risk in addition to severity and vulnerability.

4.2 Study 2 – Experiment Manipulating Threat and Efficacy

The previous study (above study 1) confirms the role of cognitive processes in both maladaptive behavior and protection behavior. However, to further examine PMT in IS, and particularly the effect of the PMT variables in privacy on the Internet, an experiment was conducted which manipulated threat and efficacy in order to explain the role of these variables on the dependent variables of maladaptive behavior and behavioral intention. This is consistent with research in PMT and particularly with the Extended Parallel Process Model (EPPM) (Witte 1992), an extension of PMT.

4.2.1 Theoretical Background and Hypotheses

A fear appeal as defined by Witte (1994; p114) is, "a persuasive message that attempts to arouse the emotion fear by depicting a personally relevant and significant threat and then follows this description of threat by outlining recommendations presented as feasible and effective in deterring the threat." Fear appeals have been studied in health related research since 1953 (Janis and Feshbach 1953) and they have been investigated in a variety of models, i.e. PMT (Rogers 1975), EPPM (Witte 1992), and the Health Belief Model (Hochbaum et al. 1952). Research in this field typically manipulates levels of both threat and efficacy in order to measure the changes in attitude, intention, or behavior.

While these models study the effect a fear appeal has on behavior change (message acceptance), there is a lack of research on which cognitive processes predict maladaptive behavior (message rejection) (Witte 1992). Therefore, EPPM addresses this gap in research by explaining that for behavior change to take place fear is a necessary condition, and *only* once fear is initiated will

behavior change take place[7]. This is different than PMT since PMT expects that threat and efficacy will *both* effect maladaptive *and* adaptive coping. EPPM explains, if there is fear, *and* the individual feels that the recommended response will be effective (response efficacy) in protecting them from the harmful event, then they will have an adaptive response (what is called in EPPM a danger control responses). However, if there is fear and the individual does *not* feel that the recommended response will be effective in protecting him then he will have a maladaptive response (what is called in EPPM a fear control response). Last, without fear there will be no response.

As discussed above in § 3.3, threat refers to the seriousness of the risk and the probability of its occurrence, while efficacy refers to the perceived effectiveness of the recommended solution and the perceived capability of performing this recommendation. In PMT and EPPM research, when the effect of a fear appeal is investigated, threat is usually an averaged measure of severity and vulnerability, and efficacy beliefs are an averaged measure of self efficacy and response efficacy. Both threat and efficacy are measured with regard to their effect on both maladaptive response (i.e. Rippetoe and Rogers 1975, Witte 1994, Witte et al. 1996, McMath and Prentice-Dunn 2005), and behavioral intention (i.e. Rippetoe and Rogers 1975, Sturges and Rogers 1996, Arthur and Quester 2004, Witte 1994, Witte et al. 1996, McMath and Prentice-Dunn 2005, Johnston and Warkentin 2010).

Results for research on fear appeals are mixed. For example, Sturges and Rogers (1996) and Rippetoe and Rogers (1975) both find that fear appeal has a significant effect on intentions only

[7] Threat is defined as a risk or danger present in a situation whether or not we are cognizant of it, while fear is a cognitive reaction that is aroused when threat is perceived (Witte, 1996)

when efficacy is high. Rippetoe and Rogers (1975) also find that people with high threat and low efficacy perceptions are more likely to have a maladaptive response. This result supports EPPM. However, Arthur and Quester (2004) only find an effect for threat (and not coping); they find that individuals exposed to a threatening message will intend to protect themselves regardless of the efficacy. Boer and Seydel (1996) found the opposite of Artur and Quester (2004). They found that intentions are increased by increasing only *efficacy* not *threat*. Last, McMath and Prentice-Dunn (2005) found that threat only had an effect on intentions not maladaptive behavior.

Witte and Allen (2000) conduct a meta-analysis of research on PMT and EPPM to determine which model is a better predictor of maladaptive *and* adaptive behavior. They find strong support for the fact that strong fear appeals are more persuasive than weak fear appeals. In addition, strong fear appeals and high levels of response efficacy produce the highest level of behavior change (i.e. danger control response), whereas strong fear appeals and low levels of response efficacy produce the highest levels of maladaptive response (i.e. fear control response). However, the meta-analysis failed to adequately explain the low threat conditions. They also failed to prove that there would be no differences in persuasion between the high threat low efficacy condition and any of the low threat conditions.

In Information Systems research, as indicated above there are a few studies that draw on PMT (Workman et al. 2008, Chenoweth et al. 2009), however, only one study that was found that conducts an experiment manipulating any of the PMT variables. Johnston and Warkentin (2010) investigate the effects of a fear appeal on behavior change in complying with information

security recommendations. However, their fear appeal manipulates severity, vulnerability, self efficacy, and response efficacy all at once. The study conducted here is a more classic design of fear appeal research where threat and efficacy are manipulated separately which is more useful in analyzing the means between the four conditions and helps to investigate the effect fear and efficacy have on each group. In addition, this study also measures maladaptive coping *and* intentions in order to verify which conditions are most likely to adopt the recommended response, and which conditions are most likely to reject the message and therefore initiate maladaptive coping. In this study the threat is an Internet privacy threat – identity theft, and the effective recommended responses are performing a credit check and using security software.

The support for the main effects (hypotheses 1, 2, 4, 5) are the same as for the survey above (see § 3.3) and are based on significant findings in previous PMT research. The interaction effects (hypotheses 3, 6, 7) are based on findings in PMT and EPPM. Both PMT and EPPM predict that threat and coping variables will interact, where behavioral intention will be initiated when threat and efficacy are high. In addition, high levels of threat and efficacy should produce the highest intention, and low levels should produce the smallest intention. For example, as indicated above Sturges and Rogers (1996), Rippetoe and Rogers (1975), and Witte (1994, 1996) all find this to be the case. With regard to maladaptive behavior, the EPPM indicates that maladaptive behavior will be initiated when threat is high and efficacy is low.

Hypothesis 1: There will be a main effect for threat on behavioral intention to perform a credit check
Hypothesis 2: There will be a main effect for efficacy on behavioral intention to perform a credit check
Hypothesis 3: There will be an interaction effect between threat and efficacy on behavioral intention to perform a credit check

Hypothesis 4: There will be a main effect for threat on behavioral intention to use security software

Hypothesis 5: There will be a main effect for efficacy on behavioral intention to use security software

Hypothesis 6: There will be an interaction effect between threat and efficacy on behavioral intention to use security software

Hypothesis 7: There will be an interaction effect between threat and efficacy on maladaptive behavior

Since EPPM proposes that adaptive responses are initiated when threat is high and efficacy is high and that maladaptive responses are initiated when threat is high and efficacy is low, this means that the fear appeal will produce *either* an adaptive response *or* a maladaptive response. Therefore, these responses will be inversely correlated since individuals will initiate *either* one *or* the other and "the two responses cancel each other out" (Witte and Allen 2000; p601).

Hypothesis 8: Behavioral intentions and Maladaptive Behavior will be negatively correlated

4.2.2 Procedure

Data was collected in a large northeastern university in the United States in February, 2011. Subjects were required to complete the survey as part of their course requirements, as such subjects self-selected and the sample was a convenience sample. The experiment took place in a lab. Subjects were randomly assigned to the 4 conditions, which resulted in an approximately equal number of subjects per cell (37 in three of the cells, and 39 in one cell).

In this study both threat and response efficacy (RE) were manipulated with essays, which is consistent with PMT research. RE is a measure of the perception of the effectiveness of the recommended response in preventing the threat or risk. For example in health related PMT

research, it has been applied in the context of the effectiveness of wearing sunscreen as a preventive measure against skin cancer (Prentice-Dunn et al. 2009). In IS research, it has been measured in the context of spyware protection behavior (Chenworth et al. 2009) and technology adoption (Johnston and Warkentin 2010). In this experiment, response efficacy is a measure of the perception of effectiveness of ID protection measures (i.e. installing security software, performing a credit check) in protecting the users' identity (i.e. from ID theft).

Before reading the manipulation essays, the subjects answered demographic questions. Severity, vulnerability, response efficacy, self efficacy and fear were also measured before the manipulation. Subjects then read the threat message, and then fear was measured again. Then, they read the response efficacy message and severity, vulnerability, response efficacy, self efficacy and fear were measured once more, followed by the dependent variables. As such fear was measured three times and severity, vulnerability, response efficacy and self efficacy were each measured twice.

The high threat essay emphasized the large amount of people (15 million) who are victims of identity theft and all the damage it can cause. For low threat they were told that only 3% of Americans are victims of identity theft. (Both of these numbers were in fact true, but the presentation emphasizes either high or low threat). The essay for High RE emphasized the effectiveness of ID protection measures such as conducting a credit check and installing security software in protecting users' information. For example, the essay explains that there are two effective measures a user can take in order to protect themselves from a security breach: installing security software and getting a credit check. The essay for Low RE emphasized that

the above two measures are actually not that effective (i.e. hackers can still breach a system). (See appendix E for essays)

4.2.3 Data Analysis

A total of 150 students were recruited. This research targeted students since individuals between the ages of 20 and 40 are most likely to have their identity stolen[8]. In this sample about 86% are between the ages of 18 – 25. This sample is split evenly between males (49 percent) and females (51 percent). For all demographics see Table 11: Subject Demographics.

Table 11: Subject Demographics

Variable	Frequency (%)	Variable	Frequency (%)
AGE		**EDUCATION**	
18-25	130 (86.6%)	Freshman	3 (2%)
Over 26	5 (.3%)	Sophomore	100 (66.7%)
Undisclosed	9 (6%)	Junior	37 (24.7%)
		Senior	6 (4%)
GENDER		BA	4 (2.7%)
Male	74 (49.3%)		
Female	76 (50.6%)		

Most constructs were measured using previously validated multi-item scales (see Appendix F) which were adapted to this context when necessary. All scales were seven point likert scales. Table 12: Principal components analysis with Varimax rotation, shows the principal components analysis with varimax rotation. The results show good discriminant and convergent validity other than for MAL3 which was dropped from further analysis. Reliability measures indicate Cronbach's alphas above the threshold of .7 (Nunally 1978), which indicates the measures are reliable (see Table 13: Reliability).

[8] http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf

In order to ascertain the successful manipulation of both threat and efficacy two dummy variables were created: Efficacy and Threat. The threat and efficacy variables were averaged[9] in a MANOVA analysis using PASW software to verify that the threat variables (severity, vulnerability, and threat) have a significant effect on threat only and that the efficacy variables (self efficacy, response efficacy) have a significant effect on efficacy only. These results are displayed in Table 14: Manipulation Check MANOVA.[10]

Table 12: Principal components analysis with Varimax rotation			
	1	2	3
MAL1	.029	-.249	**.752**
MAL2	-.046	.123	**.847**
MAL3	.411	.025	**.236**
MAL4	-.067	-.078	**.776**
BISS1	.221	**.895**	-.094
BISS2	.208	**.865**	-.084
BISS3	.314	**.881**	-.011
BICC1	**.900**	.257	-.161
BICC2	**.893**	.306	-.076
BICC3	**.884**	.324	-.140
MAL=maladaptive behavior, BISS=behavioral intention to use security software, BICC=behavioral intention to perform a credit check; MAL3 dropped from further analysis			

To test for main and interaction effects a MANOVA was performed[11] with maladaptive behavior, behavioral intention to use security software and behavioral intention to perform a credit check as dependent variables. There was a significant interaction effect for maladaptive behavior $F(1, 146) = 4.510$ at the $p<.05$ level, but no significant main effect. For behavioral intention to perform a credit check there was a main effect for threat, $F(1, 146) = 6.07$ at the $p < .05$ level, and a main effect for efficacy, $F(1, 146) = 14.68$ at the $p < .001$ level. There were no

[9] Reliability of the averaged scales was well above the .7 threashold.
[10] A separate MANOVA analysis was also run with each averaged construct: severity, vulnerability, threat, response efficacy, and self-efficacy. The dummy threat variable had a significant effect on vulnerability and threat (not severity), and the dummy efficacy variable had a significant effect on response efficacy and self efficacy.
[11] MANCOVA results show no significant effects of the covariates: age, misuse awareness, cookie settings, use of security software, frequency of personal privacy invasion, and frequency of acquaintance privacy invasion.

significant main or interaction effects for behavioral intention to use security software (see Table 15: MANOVA Results). These results do not support hypotheses 3, 4, 5, and 6.

Table 13: Reliability			
	Cronbach's Alpha	**Mean**	**S.D.**
Maladaptive Behavior(without Mal3)	.73	2.82	1.18
Behavioral Intention (security software)	.91	5.81	1.07
Behavioral Intention (credit check)	.96	5.17	1.39
Efficacy (averaged)	.91	5.19	.99
Threat (averaged)	.81	5.38	.79

In order to investigate the main and interaction effect the means were analyzed by plotting them on a graph (Figure 6: Maladaptive Behavior). For maladaptive behavior there is no main effect but a significant interaction. Investigating the means reveals that as threat and efficacy increase it is less likely that an individual will cope by rejecting the fear message, however, when threat is

Table 14: Manipulation Check MANOVA						
Source (IV)	Manipulation Check	Sum of Squares	DF	Mean Square	F	P value
Threat	MeansThreat	8.290	1	8.290	**14.332**	.000
	MeansEfficacy	4.147E-6	1	4.147E-6	.000	.998
Efficacy	MeansThreat	.944	1	.944	1.631	.204
	MeansEfficacy	54.954	1	54.954	**87.531**	.000
Threat*Efficacy	MeansThreat	.105	1	.105	.182	.670
	MeansEfficacy	.768	1	.768	1.224	.270

Low and efficacy is high it is more likely that individuals will initiate a maladaptive response. The HTHE condition had the smallest mean (2.53) for maladaptive behavior, and the largest mean was for the LTHE condition. This partially supports hypothesis 7, as there is an interaction effect but the direction is surprising. For behavioral intention to use security software, there were no significant effects, and when examining the means they seem to not change from condition to condition (see Table 16: Means).

Figure 6: Maladaptive Behavior

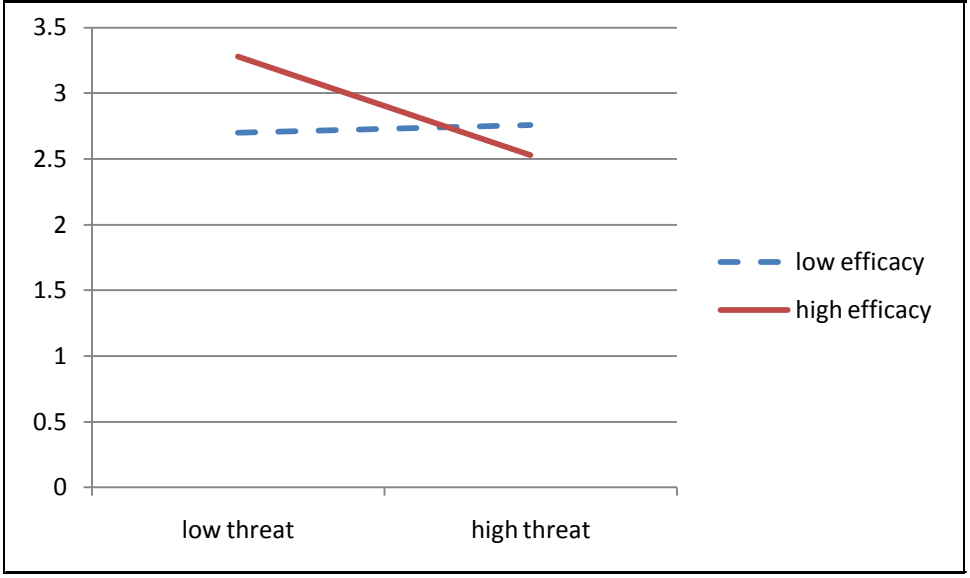


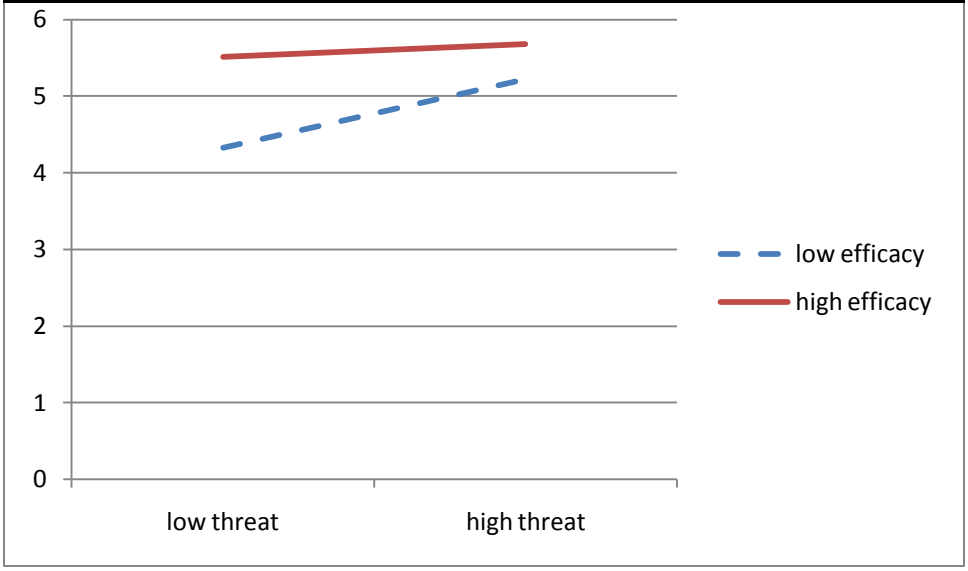
Table 15: MANOVA Results

Source	Dependent Variable	Sum of Squares	df	Mean Square	F	P value
Threat	Mal	4.465	1	4.465	3.317	.071
	Biss	.00032	1	.00032	.00028	.987
	Bicc	10.344	1	10.344	**6.066**	.015
Efficacy	Mal	1.129	1	1.129	.838	.361
	Biss	.210	1	.210	.182	.670
	Bicc	25.023	1	25.023	**14.675**	.000
Threat*Efficacy	Mal	6.070	1	6.070	**4.510**	.035
	Biss	.460	1	.460	.398	.529
	Bicc	4.966	1	4.966	2.912	.090
Error	Mal	196.508	146	1.346		
	Biss	168.543	146	1.154		
	Bicc	248.951	146	1.705		

Mal=maladaptive behavior, Biss=behavioral intention to use security software, Bicc=behavioral intention to perform a credit check

Behavioral intention towards performing a credit check had a significant main effect for both threat and efficacy, but no interaction effect supporting hypotheses 1 and 2, but not hypothesis 3. This indicates that as threat increased there was more liklihood of the individuals performing a credit check, and as efficacy increased, there was also more liklihood of the individual

Figure 7: Behavioral Intention (Credit Check)



performing a credit check. Examining the means reveals that the average for indiviudals in the Low threat condition was 4.92, and in the high threat condition was 5.45. Whereas for efficacy, the average for the low efficacy condition was 4.78 and in the high efficacy condtion was 5.6. In general, individuals in the high threat, high efficacy condition are most likely to perform a credit check, and individuals in the low threat, low efficay condition indicate the weakest intention to perform a credit check (see Figure 7: Behavioral Intention (Credit Check)).

Table 16: Means

MAL	LOW THREAT	HIGH THREAT
LOW EFFICACY	2.70	2.76
HIGH EFFICACY	3.28	2.53
BISS	LOW THREAT	HIGH THREAT
LOW EFFICACY	5.79	5.91
HIGH EFFICACY	5.82	5.72
BICC	LOW THREAT	HIGH THREAT
LOW EFFICACY	4.33	5.22
HIGH EFFICACY	5.51	5.68

To analyze hypothesis 8 a Pearson's correlation (Table 17: Pearson's correlations) was conducted. This reveals a signficant negative correlation between behavioral intention to perform a credit check and maladaptive behavior. There is no significant correlation for behavioral intention to use security software, which is not surprising concidering the lack of signficinat results for this variable in the MANOVA. A summary of hypothesis results is displayed in Table 18: Summary of Hypothesis for Study 2.

Table 17: Pearson's correlations

		mal124	biss	bicc
mal	Pearson Correlation	1		
	Sig. (2-tailed)			
	N	150		
Biss	Pearson Correlation	-.155	1	
	Sig. (2-tailed)	.058		
	N	150	150	
bicc	Pearson Correlation	**-.163***	.540**	1
	Sig. (2-tailed)	.046	.000	
	N	150	150	150

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

Table 18: Summary of Hypothesis for Study 2

H1	There will be a main effect for threat on behavioral intention to perform a credit check	Supported
H2	There will be a main effect for efficacy on behavioral intention to perform a credit check	Supported
H3	There will be an interaction effect between threat and efficacy on behavioral intention to perform a credit check	Not Supported
H4	There will be a main effect for threat on behavioral intention to use security software	Not Supported
H5	There will be a main effect for efficacy on behavioral intention to use security software	Not Supported
H6	There will be an interaction effect between threat and efficacy on behavioral intention to use security software	Not Supported
H7	There will be an interaction effect between threat and efficacy on maladaptive behavior	Supported
H8	Behavioral intentions and Maladaptive Behavior will be negatively correlated	Supported

4.2.4 Discussion

This study successfully manipulated threat and efficacy with essays in an Information Systems setting. There has not been previous research in IS manipulating both threat and efficacy individually and investigating its effects on behavioral intention *and* maladaptive coping. This study also successfully adapts PMT and EPPM research to the IS setting.

Table 19: Screening Questions	
Security Software installed?	Number of subjects (%)
Yes	121 (81%)
No	20 (13%)
Not sure	9 (6%)
Checked Credit Report?	
Yes	43 (29%)
No	101 (67%)
Not Sure	6 (4%)

The insignificant results for behavioral intention towards using security software were surprising. According to PMT and EPPM threat and/or efficacy should have at least a main effect on intentions (and an interaction). Analyzing the means reveals that there are no significant differences and when analyzing these means with a Tukey contrast analysis. While this result is puzzling, it is less alarming when investigating the response to the pre-manipulation question that measured whether the individual has security software installed on their most frequently used computer. These results are displayed in Table 19:. The vast majority of subjects (81%) have security software already installed on their computers. In addition, of the subjects who indicate that they were sure they have security software installed on their computers, 83% indicate that it is updated at least somewhat frequently. This seems to indicate that since most subjects already have security software installed, most of them update the software periodically, and the mean intention to use security software was 5.81, there was no need for the fear appeal and therefore it didn't change intentions, as it was already a frequent behavior. This is consistent with a finding in an experiment by McMath and Prentice-Dunn (2005). They find that threat

information had a stronger relationship with intentions than with maladaptive coping. They explain this surprising result by explaining that "the widespread dissemination of efficacy information … may have rendered coping appraisal manipulations less effective and more prone to ceiling effects" (p636). A similar event may have occurred here, where people are aware of the privacy threats, and the recommendation of using security software to combat it, so it becomes a non-issue.

However, with regard to behavioral intention to perform a credit check, only 29% of subjects had ever checked their credit report. Of these subjects only 13% had checked their credit within the last three months, and 42% had only checked their credit report within the last year, or over a year ago. This indicates a need for behavior change. Although a meta-analysis indicated that there were main and interaction effects on behavioral intention (Witte and Allen 2000), only main effects were found in this study, which is consistent with other research (i.e. Roskos-Ewoldsen 2004). In addition, this is consistent with PMT research which posits that individuals perform a threat and coping appraisal before they decide whether to protect themselves and both of these cognitive processes are related to subsequent actions. This study showed that in order to increase intention to perform a credit check *either* high threat, *or* high efficacy would be sufficient. This is evidenced by the fact that with a Tukey contrast, there are only significant mean differences between LTLE condition and the other three conditions ($p<.05$). While it is expected that HTHE would have the largest mean in terms of intention to perform a credit check, the mean is the largest but not significantly larger than HTLE, or LTHE conditions. It is also interesting to note that although mean differences were analyzed, in general, *all* means indicate a strong intent to perform a credit check (all are over 4 which indicated neither agree nor disagree,

as the scale was a likert scale ranging from 1-7) with LTLE condition being the lowest (as expected).

The results for maladaptive behavior indicate a significant interaction effect. A Tukey contrast analysis revealed that there was a significant difference between HTHE and LTHE ($p < .05$) conditions. These results seem to indicate that there was a difference between the threat levels only when efficacy was high, and that there was a smaller maladaptive response when threat was high as compared to when threat was low. This is consistent with research, where as threat and efficacy increase there will be less maladaptive coping. However, what was surprising was that when efficacy was low there was no significant difference in the means, an additional factor that was not expected was that the highest mean was the LTHE condition and not the HTLE condition. When analyzing the means, in general all means are below 3.3 (on a 1-7 likert scale). This seems to suggest that the maladaptive response is very low in the first place. These results also seem to support PMT as opposed to EPPM because PMT indicates that efficacy and threat are both important in the appraisal process, whereas EPPM proposes that fear (threat) is a necessary condition in order for any coping (whether adaptive or maladaptive) to take place. In this study the largest mean for maladaptive coping was the LTHE condition (not the HTLE). One possible explanation for these surprising results is that the interaction effects are complicated in PMT models especially when averaging threat and efficacy variables. There are many inconsistent results and often interactions between the variables that make up threat (severity and vulnerability) and the variables that make up efficacy (response efficacy and self efficacy (Cismaru 2006). The fact that there were no significant differences between low and high threat for the low efficacy condition can possibly be explained by the fact that most subjects had heard of identity theft (93%). The efficacy condition can serve to actually increase their

threat level fact that they are being told that these particular measures can be used (or do not work) to reduce the likelihood of identity theft, may artificially increase their perception of threat which would cause their maladaptive response to be similar.

4.3 Study 3- Experiment Manipulating Interface and Complexity

Since Online Social Networking has become such as important part of people's lives, it is important for individuals to have an understanding of their privacy settings. Research indicates that often users do not adjust their privacy settings even if they claim to have an adequate understanding of them (Debatin et al. 2009). In fact, in study 1 above (the survey) a number of subjects indicated that they have not reviewed their privacy settings, "because it takes some time" "because I don't think there is a need," "laziness," or "I don't know where to find it." This indicates that although users seem to think they understand privacy settings, their actions indicate that they don't have a full understanding of all the privacy issues (Debatin et al. 2009). Therefore, in this study this need is addressed by designing an interface that should be more intuitive and easier to use and understand.[12] This interface displays *both* the default or recommended settings[13] *and* the changes that the user has made to the profile. The intention is to provide the user with more information about 'safe' privacy settings while giving him a greater understanding of *his* settings in comparison to these recommended settings. The current privacy settings on Facebook do give the user control over his information, however, the user must go through *multiple* screens in order to adjust all the settings and there is no information about default or recommended settings in comparison to the users' actual settings.

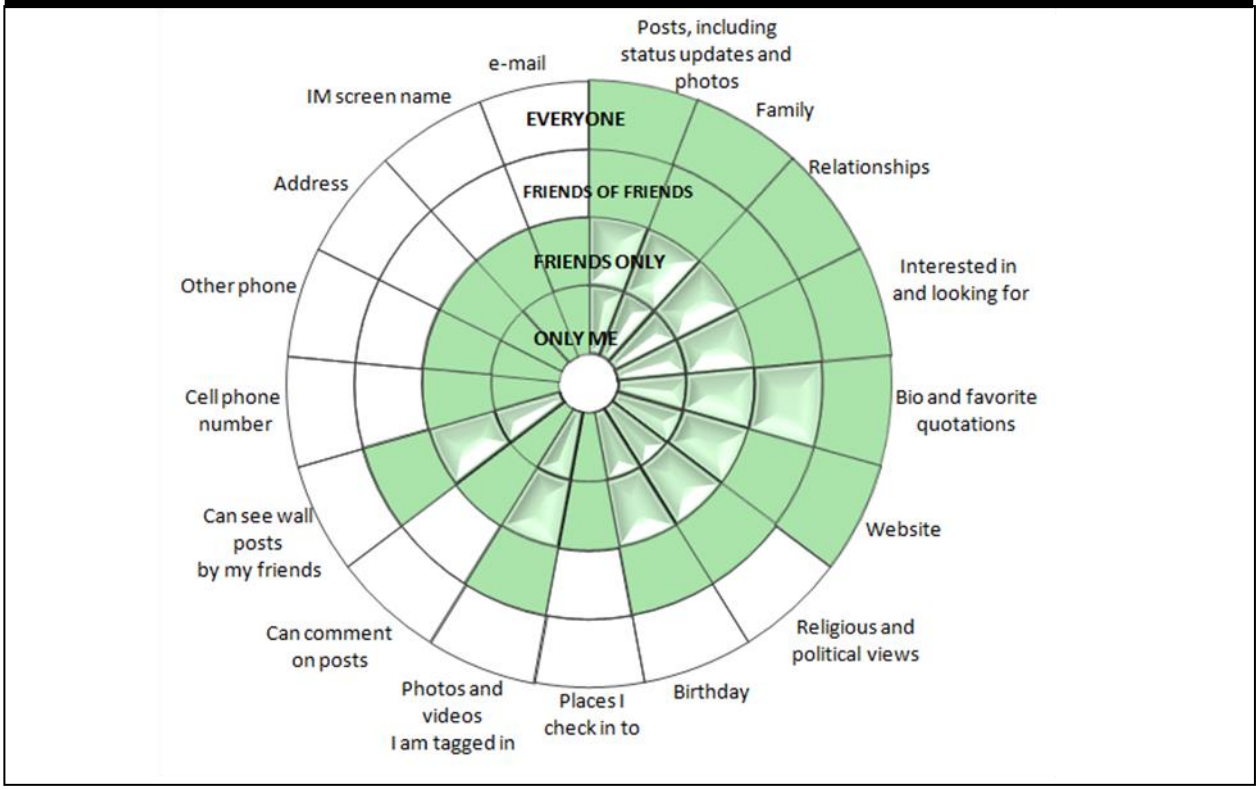
The figure below (Figure 8: Wheel interface1) depicts one of the user profiles using the new wheel interface. The categories that the user can change are displayed around the wheel. The inner most ring indicates a setting of 'only me', the next ring, indicates a privacy setting of 'friends only', the following ring (third from the middle) indicates a privacy setting of 'friends of

[12] The design used was based on the wheel that Privacy Defender by Reputation Defender uses.
[13] Default and recommended are used interchangeably

friends' and the outermost ring indicates a setting of 'everyone.' Any portion of the wheel that is dark green represents the recommended setting. For this study the default settings that Facebook uses were the ones used for the recommended setting. Any light green and indented piece of the wheel indicates a setting that the user has changed from the default level. For example, in this case the default for the 'family' category is 'everyone' and the user has set it to 'friends only,' and the 'e-mail' category has not been changed from the default so it is set to 'friends only.'

Figure 9: Wheel interface2 is a second user profile. Dark green remains the default, however, anything set *above* the default (meaning a less safe setting) is in red and indented. To illustrate, the 'can comment of posts' category by default is set to 'friend only' but this user has set it to 'friends of friends.'

Figure 8: Wheel interface1



For the tabular format the Facebook display format is used, however there are more categories displayed in order to match all the categories displayed in the wheel. In addition, the 'only me' category was added to match the wheel (and this is available as a Facebook custom setting). In the tabular interface two tables were displayed at a time in order to be able to show the user the default and user setting at the same time. See Figure 10: Tabular interface for one example of the tabular format.

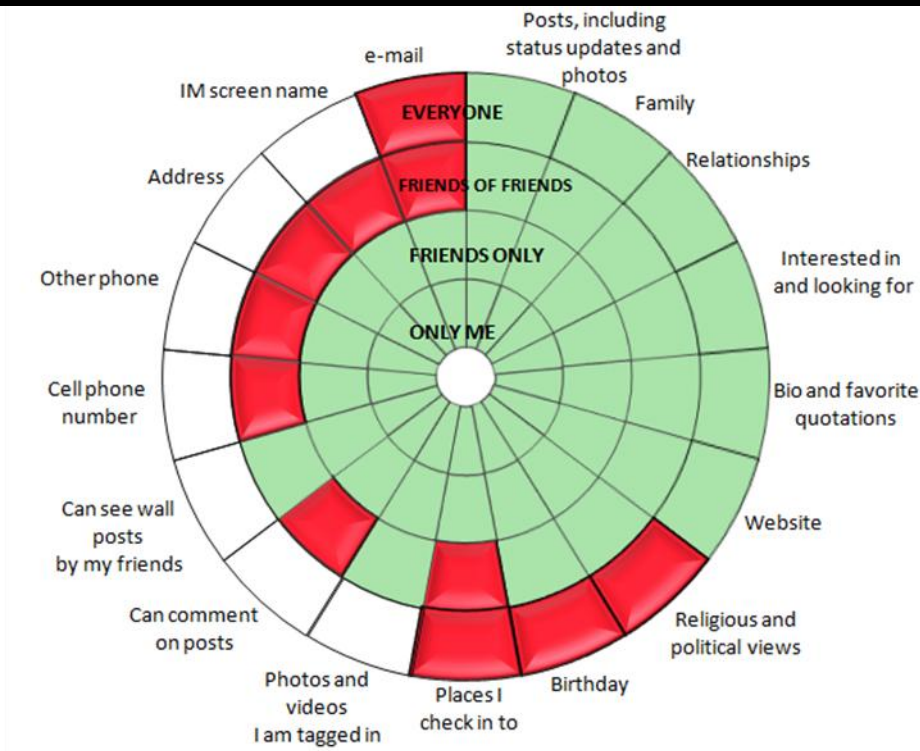
4.3.1 Theoretical Background and Hypotheses

This study is grounded in Cognitive Fit (CF) Theory (Vessey 1991, Vessey and Galletta 1991), which investigates information presentation and the associated effects on performance. CF theory is based on Task Technology Fit (Zigurs and Buckland 1998). Both these theories explain that task demands and display format are very important when designing displays since the presentation format influences decision strategies, the cognitive costs and benefits of the interface (Jarvenpaa, 1989), and performance (Bettman and Zins 1989). Additionally, mismatches between data representation and the task can slow down decision making (Vessey, 1991). According to CF theory, when individuals are presented with a task, they form a mental representation of the problem. When the *problem* representation matches the *mental* representation there is cognitive fit, which leads to effective and efficient problem solving. However, when there is a mismatch between the *problem* and *mental* representation, the individual needs to transform the data to fit his mental representation, which will result in greater cognitive effort and lower performance.

A number of studies have investigated the use of information visualization techniques in helping users comprehend information and increase task performance. (i.e. Carter 1947, Xiang et al.

2005). In general, research has attempted to create a framework to identify which type of interface combined with a specific task type will enhance performance. A number of studies

Figure 9: Wheel interface2



have investigated graphs versus table, paper versus computer screen, or multimedia representation (see Kelton et al. 2010 for a comprehensive review). Most research investigates the difference between graphical interface versus a tabular format in decision tasks and their effect on accuracy and time (i.e. Kennedy et al. 1998, Vessey 1991, Umanath and Vessey 1994, Speier 2006), and a good portion of this literature is based on the presentation of *numerical* data. Other literature uses a choice task where the organization of the many choices is by attribute or alternative (Bettman and Zins 1979, Cao et al. 2009, Kamis et al. 2006) or list versus matrix (Hong et al. 2004), and again find that CF plays a role in performance and/or enjoyment.

In addition to comparing interface types, research has also categorized types of tasks. For example, past research has found that for *spatial* tasks (i.e. looking at relationships in data or trends) graphs have greater cognitive fit, whereas, for *symbolic* task (i.e. extracting precise values) tables have greater cognitive fit (i.e. Benbasat and Dexter 1986, Stone et al. 1997, Speier

Figure 10: Tabular interface

DEFAULT

	Everyone	Friends of Friends	Friends Only	Only Me
Posts, including status updates and photos	•			
Family	•			
Relationships	•			
Interested in and looking for	•			
Bio and favorite quotations	•			
Website	•			
Religious and political views		•		
Birthday		•		
Places I check in to			•	
Photos and videos I am tagged in		•		
Can comment on posts			•	
Can see wall posts by my friends		•		
Cell phone number			•	
Other phone			•	
Address			•	
IM screen name			•	
e-mail			•	

USER A

	Everyone	Friends of Friends	Friends Only	Only Me
Posts, including status updates and photos			•	
Family			•	
Relationships			•	
Interested in and looking for			•	
Bio and favorite quotations		•		
Website			•	
Religious and political views			•	
Birthday			•	
Places I check in to			•	
Photos and videos I am tagged in			•	
Can comment on posts			•	
Can see wall posts by my friends			•	
Cell phone number			•	
Other phone			•	
Address			•	
IM screen name			•	
e-mail			•	

2006). The task complexity also has important CF implications. Task complexity has been studied relative to human information processing (Miller 1956), which posits that humans have limited amount of cognitive ability to store information. Therefore, they use heuristics to help them process large amount of information (such as 'chunking'). As task complexity increases, and hence cognitive load, people may sacrifice their performance (in terms of time and/or accuracy) in exchange for cognitive effort (Todd and Benbasat 1999, Speier 2006, Johnson and Payne 1985). Using a data visualization technique (such as a graph or wheel) can reduce the

cognitive load on working memory by shifting the cognitive processing to perceptual processing, which reduces the demands on memory since the human brain excels at processing images and recognizing patterns (Card et al. 1983, Wickens and Carswell 1995).

Another aspect of visual displays that reduces cognitive load is visual cues. Visual cues facilitate perceptual performance and result in higher problem solving performance (Kim et al. 2000). One example of a visual cue is color. Color coding in graphs, reduces cognitive load by facilitating 'chunking' a cognitive processing method that individuals use to help reduce cognitive effort in memory (Miller 1956). Color coding reduces cognitive effort, by forming perceptual groups since it helps to highlight the differences in groups of information on the display, thereby reducing similarity (Lohse 1997, Treisman 1982). In fact, research has shown that information searching with color is faster in some situations (Carter 1982, Treisman 1982, Benbesat et al. 1986).

In this experiment a wheel (with color) is compared to a table (black and white) for displaying privacy settings. Simple and complex questions were also compared. According to Wood (1986) a complex task is defined in part by the number of processes that needs to be executed, and a higher level task requires interpretation and analysis before reaching a conclusion (Jarvenpaa and Dickson 1988). The complex questions in this study were designed so that they required higher level information processing that involves and multiple comparisons and steps in order to reach a conclusion. The simple questions did not involve any comparisons and required only focusing on one particular piece of information in the display. Therefore, for simple questions tasks there is little cognitive effort required and therefore a difference is not expected

for time or for accuracy. However, because of the higher level processing required for complex questions they will take more time to complete.

H1: There will be a main effect of complexity on time. As the complexity of the questions increases, the time taken to answer will also increase.

H2: There will be a main effect of complexity on accuracy. As the complexity of the questions increase the accuracy of the answers will decrease.

The complex questions require comparisons in the information displayed and recognition of patterns. Therefore, the wheel, which displays information with color, to help group categories, and displays information spatially should require less cognitive effort and therefore lead to higher accuracy and less time to complete. The wheel interface also reduces cognitive load by displaying all pertinent information in one display so that the user does not have to compare two different charts (like in the table). Therefore, the wheel interface should generally take less time to answer questions.

H3: There will be a main effect of graph type on time. The time taken to comprehend information using the wheel will be less than that for the table

H4: There will be a main effect of graph type on accuracy. The accuracy of the answers using the wheel will be greater than the accuracy than that for the table.

H5: There will be an interaction effect between complexity and graph type on time. As complexity increases, the time taken to answer questions using the table will increase more rapidly than that for the wheel.

H6: There will be an interaction effect between complexity and graph type on accuracy. As complexity increases, the accuracy of the answers will decrease more rapidly for the table than that for the wheel.

4.3.2 Procedure

The study took place in a large Northeastern University in a lab. The subjects were required to participate as part of a course requirement. This study took place in multiple sessions with approximately 10 students in each session. The entire experiment was hosted on an online survey website. When all subjects were present, they answered basic demographic information. Then the researcher gave a training session with Microsoft PowerPoint that included screenshots of sample user profiles using both the wheel interface and the tabular interface. These profiles were similar to the actual profiles the subjects saw when they completed the experimental manipulation. After the training session the subjects, together with the researcher, completed training questions that were similar in format to the actual questions used in the study. The researcher displayed the question with a projector in the front of the lab and the subjects followed along on their own screen. Immediately following the training the subjects completed the study.

The study had a 2 x 2 experimental design manipulating interface (wheel vs. table) and complexity (simple vs. complex), within-subjects, so each subject completed all manipulations. Subject were shown a screenshot of a user's profile (similar to figures 8 - 10 above), they then had to answer questions that would indicate comprehension of the settings. In order to control for order, subjects were randomly assigned to an identical study where either wheel was first, or table was first. In both versions subjects started with simple questions and then completed the complex questions. The questions for both the wheel and the table were the same, and there were nine simple questions (i.e. that asked only about default or user settings) and 11 complex questions (i.e. where subjects needed to compare settings or profiles). See appendix G for all

questions used and appendix H for all user profiles used. After completing all questions, they answered questions about ease-or-use, comprehension, and enjoyment.

4.3.3 Data Analysis

A total of 67 students were recruited. In this sample about 79% are between the ages of 18 – 25. This sample is split between males (46 percent) and females (54 percent). For all demographics see Table 20: Subject Demographics.

The data was analyzed with PASW using the GLM repeated measures procedure. Accuracy was measured by summing the number of questions answered correctly and then converting this to a percent since there were an unequal amount of questions for simple and complex conditions. Results for Accuracy are displayed in Table 21: Test of within subjects contrasts for ACCURACY below. There was a significant main effect for interface $F(1, 66)=.11$ at the $p<.05$ level. There was a significant main effect for Complexity $F(1, 66)=.23$ at the $p<.001$ level, and a significant interaction effect $F(1, 66)=.1$ at the $p<.001$ level. On average, users were correct using the wheel interface 89% of the time, and using the table they were correct 93% of the time.

Table 20: Subject Demographics

Variable	Frequency (%)	Variable	Frequency (%)
AGE		**EDUCATION**	
18-25	53 (79.1%)	Sophomore	49 (73.1%)
Over 26	6 (9%)	Junior	15 (22.4%)
Undisclosed	8 (11.9%)	Senior	3 (4.5%)
GENDER			
Male	31 (46.3%)		
Female	36 (53.7%)		

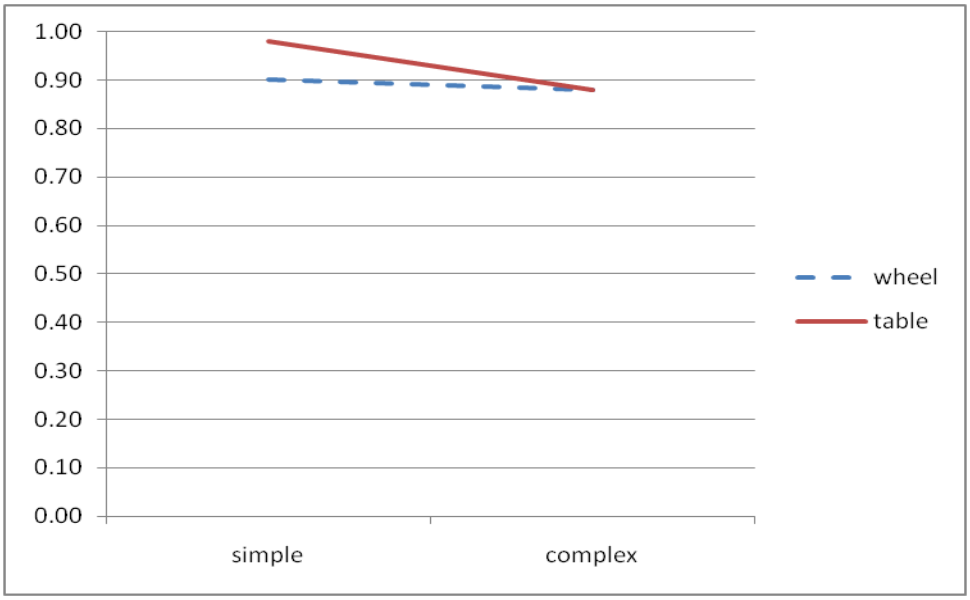
Whereas, on simple questions they were correct 94% of the time and on complex questions they were only correct 88% of the time. These percentages are all high indicating that for the subjects

got a large majority of all questions correct. See Figure 11: ACCURACY below for the plot of the four cells (simpleWheel, complexWheel, simpleTable, complexTable).

Table 21: Test of within subjects contrasts for ACCURACY					
Source (IV)	Sum of Squares	df	Mean Square	F	P value
interface	.110	1	.110	**5.960**	.017
Error(interface)	1.216	66	.018		
complexity	.255	1	.255	**18.175**	.000
Error(complexity)	.927	66	.014		
interface * complexity	.103	1	.103	**12.391**	.001
Error(interface*complexity)	.546	66	.008		

Post hoc tests were conducted to further examine the significant main and interaction effects. Using the Bonferroni correction reveal that there is a statistically significant difference in accuracy between the interfaces ($p<.001$) and complexity ($p<.001$). Post hoc tests using Tukey to contrast means between the groups indicates that there is a significant difference between wheel and table for simple questions ($p<.05$) and between simple and complex questions for the table interface ($p<.001$). These results indicate that there is a significant difference in the number of questions the subjects answered correctly using the table interface, where simple questions are more likely to be answered correctly. In addition, there is no statistical difference between the two interfaces for complex questions. To summarize, subjects answered more questions correctly for the table interface when the questions were simple, however, for the more complex questions the accuracy was the same, so there was a significant decrease in the number of questions answered correctly for the tabular interface. These results support Hypothesis 2, and Hypothesis 6, but not Hypothesis 4.

Figure 11: ACCURACY



Time was measured by displaying one question at a time per screen in the survey and timing how long before user clicked to advance to the next screen (after answering). Results for Time are displayed in Table 22: Test of within subjects contrasts for TIME below. There was a significant main effect for interface $F(1, 66)=5.48$ at the $p<.05$ level. There was a significant main effect for Complexity $F(1, 66)=610.81$ at the $p<.001$ level, and a significant interaction effect $F(1, 66)=29.06$ at the $p<.001$ level. On average, users took 22 seconds to answer questions were using the wheel interface, and using the table they took an average of 24 seconds. For simple questions they took an average of 13 seconds to answer, and they took an average of 33 seconds to answer complex questions. See Figure 12: TIME below for the plot of the four cells (simpleWheel, complexWheel, simpleTable, complexTable).

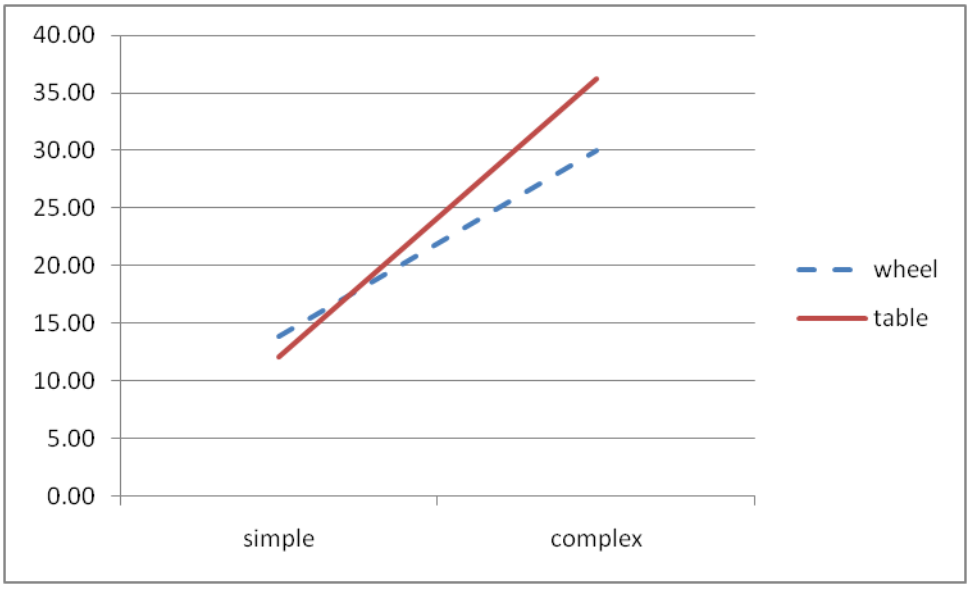
Post hoc tests were conducted to further examine the significant main and interaction effects. Using the Bonferroni correction reveal that there is a statistically significant difference in

accuracy between the interfaces (p<.001) and complexity (p<.001). Post hoc tests using Tukey to contrast means between the groups indicates that all mean differences are significant at the p<.001 level besides for the difference between the time it took to answer simple questions for the wheel versus the table interface. These results indicate that in general, simple questions took less time to answer than complex questions. However, for the tabular interface simple questions the table did not take a significantly less amount of time, whereas for complex questions it did.

Table 22: Test of within subjects contrasts for TIME

Source (IV)	Sum of Squares	df	Mean Square	F	P value
interface	340.165	1	340.165	**5.476**	.022
Error(interface)	4099.835	66	62.119		
complexity	27204.579	1	27204.579	**610.806**	.000
Error(complexity)	2939.561	66	44.539		
interface * complexity	1049.087	1	1049.087	**29.064**	.000
Error(interface*complexity)	2382.333	66	36.096		

Figure 12: TIME



These results support Hypothesis 1, Hypothesis 3, and Hypothesis 5,. See Table 23: Hypotheses for interface experiment below for a summary of hypothesis results.

Table 23: Hypotheses for interface experiment

H1	There will be a main effect of complexity for time. As the complexity of the questions increases, the time taken to answer will also increase.	Supported
H2	There will be a main effect of complexity for accuracy. As the complexity of the questions increase the accuracy of the answers will decrease.	Supported (only for table)
H3	There will be a main effect of graph type. The time taken to comprehend information using the wheel will be less than that for the table	Supported
H4	There will be a main effect of graph type. The accuracy of the answers using the wheel will be greater than the accuracy than that for the table.	Not Supported
H5	There will be an interaction effect between complexity and graph type. As complexity increases, the time taken to answer questions using the table will increase more rapidly than that for the wheel.	Supported
H6	There will be an interaction effect between complexity and graph type. As complexity increases, the accuracy of the answers decrease more rapidly for the table than that for the wheel.	Supported

After answering the comprehension questions, the subjects were also asked to compare the two interfaces and to indicate with a 5 point bi-polar scale which interface they found easier to use, and more enjoyable (see Table 24: Comparing tables to below) where table was anchored at 1 and wheel was anchored at 5. The results indicate that for ease-of-use, comprehension, and preference subjects seem to be indifferent (all results are approximately 3). However, for fun and enjoyable, subjects preferred the wheel.

Table 24: Comparing tables to wheel*	
Easier to use	2.95
More difficult to use	2.98
Useful	3.09
Improve comprehension	2.95
Increase comprehension	2.95
Understandable	3.09
More frustrating	2.89
More confusing	3.02
Preferable to use	3.03
Fun	3.70
Enjoyable	3.42
*table was anchored at 1 and wheel was anchored at 5	

4.3.4 Discussion

This study contributes to cognitive fit theory by applying this theory in the context of a privacy setting interface. Similar to other CF studies the task type was manipulated (simple vs. complex questions) and the Interface type was manipulated (table vs. wheel). The findings partially support cognitive fit theory since only for one performance measure (time) the wheel excelled, whereas for accuracy there was no significant difference between the two interfaces for complex questions. This finding is actually in line with other CF studies, where time was significantly different for two interfaces, but not accuracy (Benbasat and Dexter 1986, Dickson et al. 1986), and in general depending on the type of task and type of interface results have been mixed (Vessey, 1991). Examining all results this study finds that for simple tasks the table was more accurate, however in this case the wheel was a brand-new representation of the data for these subjects so the significant difference in accuracy between table and wheel can be a matter of familiarity with the interface. What is more interesting here, is that for complex tasks the accuracy was the same, but when using tables subjects were statistically significantly *less* accurate for complex tasks, whereas when using the wheel there was no significant difference in

accuracy when comparing the two task types. Therefore, more research is needed in this area as there is a chance that with more familiarity or with more complex questions accuracy would be better for the wheel.

The second measure of performance, time, has results that were entirely in line with CF. The hypotheses that complex questions would take significantly more time and that as using the wheel interface the subjects would take significantly less time to answer the questions were confirmed. In addition, as the questions got more complex the wheel interface took significantly less time to answer, because there was less cognitive effort required based on the graphical and colorful interface. In short, for complex questions subjects got the same amount of questions correct, but it took them less time to get their answers using the wheel interface. Although CF was not confirmed for both performance measures, the finding are still interesting and do show that the type of interface can decrease cognitive load (time). In this case accuracy probably suffered because of the novelty of the wheel interface, and although subjects did not seem to prefer one interface over the other in terms of comprehension and ease-of-use, they thought the wheel was more enjoyable and fun to use.

Chapter 5

Conclusions and Future Research

This research examined privacy in the Online Social Networking context and built a model explaining protection behavior and maladaptive behavior on an OSN. The model used the PMT cognitive process variables such as benefits, costs, response efficacy, and self efficacy to measure their effect on protection behavior and maladaptive behavior. In addition, instead of measuring severity and vulnerability as they are commonly measured in PMT research, this study measured perceived privacy risk and modeled severity and vulnerability as antecedents to perceived privacy risk. Trust, privacy disposition, and awareness were also measured as privacy risk antecedents. The survey results were analyzed using SmartPLS and found overwhelming support for the model, where the privacy risk antecedents explained 55% of the variance in perceived privacy risk and the cognitive mediator variables accounted for about 30% of the variance in both maladaptive behavior and protection behavior.

This study contributes to PMT by extending its use to the privacy context with a special focus on Online Social Networking. It also contributes to the Social Exchange Theory (SET) and finds that in this context the costs determine both maladaptive and protection behavior response, whereas benefits only determine protection behavior. In addition, the results also contribute to research on OSN since most research in OSN has been geared towards identifying motivations of OSN use and examining the types of information disclosed, but fails to explain protection behavior (or lack thereof). Last, the results validate the use of perceived privacy risk as part the PMT model in place of severity and vulnerability as a cognitive mediator. This research is novel in that it explores the role of privacy antecedents on both maladaptive and adaptive behaviors in a single model with the PMT cognitive process variables as mediators.

In this study, benefit and protection intention were measured as reflective concepts. Future research should examine both these measures as formative constructs since they can be multi-faceted. For example, a benefit of OSN is also finding old friends, and playing games online. In addition, future research should address the proposed interaction effects and attempt to model the interaction with a simpler model in order to have adequate power to be able to examine them.

In addition to testing the PMT model with a survey, this research also explored the impact of core variables – threat and efficacy – experimentally. A 2 x 2 experiment was conducted by manipulating threat and efficacy in order to causally test their relationship with adaptive and maladaptive behaviors. Research in IS has not addressed the manipulation of threat and efficacy variables in the privacy context. A recent study (Johnston and Warkentin 2010) used fear appeal to investigate its effect on behavior change with regard to anti-virus software but this research bundled threat and efficacy together. In my experiment, threat and efficacy were manipulated separately with two levels each, which is consistent with the Extended Parallel Process Model (EPPM). This successful manipulation of threat and efficacy in and of itself is a contribution to IS research as response efficacy and self efficacy are usually seen as individual's perceptions that remain stable. This research found that either high threat *or* high efficacy level were sufficient for an individual to initiate protection intentions. For maladaptive behavior, the results are in line with EPPM where individuals who read the high threat high efficacy essay were least likely to initiate maladaptive behavior. Last, as indicated by EPPM, since an individual will choose either a maladaptive response or protection intention, these two coping behaviors were negatively correlated.

In order to investigate the effects of threat and efficacy on protection and maladaptive behavior, this study looked at the broader phenomenon of online identity theft. Future research should look at narrower protection realms such as protection of financial information. In addition, this research investigated a general measure of maladaptive behavior; however other PMT and EPPM studies have measured other facets of maladaptive behavior such as hopelessness and avoidance. Future research should incorporate these other facets of maladaptive behavior.

The last study examined two different interfaces for privacy settings. The goal of the previous two studies was to explain user behavior with regard to protection. However, an important aspect of protection behavior is the use of a privacy setting interface. The privacy settings currently used by OSN (such as Facebook) is not necessarily intuitive to use and can be quite frustrating for the user since they are usually displayed on multiple screens. Therefore, users may find it difficult to actually use them and to fully understand the implications of their privacy settings. A better designed interface would make using privacy settings more enjoyable, engaging and fun. It would also help the user comprehend what their privacy settings are set it and the safety of their settings. Therefore, this study designed a new privacy settings interface, one that displays information about the recommended ('safe') settings in addition to the user's settings by utilizing a color coded wheel. This study used a 2 x 2 experimental within-subjects design to compare two interfaces (wheel versus table) by evaluating the differences in comprehension for two levels of information complexity (simple versus complex). The tabular interface was similar to the privacy settings currently used by Facebook. Both of the interfaces displayed the recommended ('safe') settings in addition to the user's settings simultaneously on the same screen. The results of our study supported Cognitive Fit theory. The graphical interface

(wheel) was superior to the tabular interface for performance vis-à-vis time. For the second performance variable of accuracy, the tabular interface took less time for simple questions, but not for complex questions. These results contribute to research on interface design in privacy research. The results also have implications for interface design in OSN in creating an interface that can incorporate information to assist the user in choosing appropriate and safe settings. Future research should measure how individuals interact with the interface and investigate the differences in the way users set their privacy settings with each interface. In addition, it should measure perceptual measures such as self efficacy, control and enjoyment in order to make practical suggestions for improving interface design on OSN.

All three studies share the limitation of using students as participants. Although this demographic makes up a large part of the OSN population there has been a recent trend towards older individuals (30+) using OSN. It would be interesting to see if any of these results would change for these older (and possibly less experienced) computer users.

In conclusion, this research examined privacy on OSN from multiple perspectives. It established the role of privacy risk antecedents and PMT in predicting protection behavior and maladaptive behavior. It also examined the use of a fear appeal in changing individual's behavior with regard to identity theft. Last, it designed and tested a novel, improved interface for privacy settings.

APPENDIX A: Survey Instrument Study 1

All scale items are 5 point likert scales ranging from strongly agree (1) to strongly disagree (5)

RISK ANTECEDENTS	
	TRUST IN ONLINE SOCIAL NETWORK (Dinev and Hart 2006)
TRUST1	Online social networks are safe environments to exchange information with others
TRUST2	Online social networks are reliable environments
TRUST3*	Online social networks handle personal Information submitted by users in a competent fashion
	AWARENESS (Dinev and Hu 2007)
AWARE2	I follow the news and developments about the privacy issues and privacy violations.
AWARE3	I keep myself updated about privacy issues and the solutions that companies and the government employ to ensure our privacy
AWARE5	I read about the problems of privacy invasion on OSNs
AWARE6	I discuss with friends and people around me security issues of OSNs
	VULNERABILITY
VUL1	It is highly likely that my personal information could be inappropriately used by online social networks
VUL2	The chances are high that the information I share in the online social network could lead to a privacy breach
VUL3	It is highly likely that the information I share in the online social network could be accessed by others without my knowledge
VUL4	The chances are high that the information I share in the online social network could be seen by others without my permission
	SEVERITY
SEV1	A privacy breach in my OSN could pose a serious problem for me
SEV2	If others improperly access my information on OSN, it could impact my reputation significantly
SEV3	If others see my information on the online social network without my permission, it could embarrass me severely
	PRIVACY DISPOSITION (Xu et al. 2009)
DISP1	Compared to others, I am more sensitive about the way my personal information is handled
DISP2	To me, it is the most important thing to keep my personal privacy
DISP3	Compared to others, I tend to be more concerned about threats to my personal privacy
COGNITIVE MEDIATORS	
	RESPONSE EFFICACY (Witte et al. 1996)
RE1	Using privacy settings works in preventing a privacy breach
RE2	Using privacy settings is effective in preventing a privacy breach
RE3	If I use privacy settings I am less likely to have my privacy violated
	SELF EFFICACY (Armitage et al. 1999)
SE1	I believe I have the ability to use privacy settings
SE2	I am capable of using privacy settings on my OSN
SE3	I am confident I am able to use privacy settings on my OSN
SE4	If it were entirely up to me, I am confident that I would be able to use privacy settings on my OSN

	COST
COST1	It is inconvenient to change privacy settings on my OSN
COST2	It would take too much time to change privacy settings on my OSN
COST3	It would take too much effort to change privacy settings on my OSN
	PERCEIVED PRIVACY RISK (Malhotra et al. 2004 items 1-5)
RISK1	In general, it is risky to share information on an online social network
RISK2*	There would be high potential for loss associated with sharing information on an online social network
RISK3	There would be too much uncertainty associated with sharing information on an online social network
RISK4	Sharing information on an online social network would involve many unexpected problems
RISK5*	I would feel safe sharing information on an online social network'
RISK6	Sharing my information on the online social network poses a threat to my privacy
RISK7	Sharing my information on the online social network is potentially dangerous
RISK8	Sharing my information on the online social network could compromise the safety of my information
	BENEFIT
BEN1	Using online OSN allows me to stay in touch with others.
BEN2	Using online OSN enables me to reconnect with my friends
BEN6	I will be able to keep track of my friends by using OSN
BEN9	Using OSN allows me to learn more about my friends
DEPENDENT VARIABLES	
	MALADAPTIVE BEHAVIOR (Cho and Salmon 2006)
MAL1	Given what I know about privacy invasion, I sometimes feel it's almost useless to try to protect my privacy
MAL2	When I think about privacy invasion, I sometimes feel like saying, 'What's the use in protecting my privacy?
MAL3	In this day and age, it sometimes seems a hopeless task to stay protect my privacy
	PROTECTION BEHAVIOR
PB5	I changed the privacy settings on my social network to fine tune how I shared information with others.
PB6	I haven't looked at the privacy settings on my online social network thus far'
PB7	I have changed the default settings on my OSN account
*dropped item 'reversed	

APPENDIX B: Cross Loading Study 1

Cross Loadings												
	AWARE	BENEFIT	COST	MAL	PB	DISP	RE	RISK	SE	SEV	TRUST	VUL
AWR2	**0.83**	0.05	0.02	0.06	0.22	0.36	0.15	0.17	0.15	0.14	0.05	0.11
AWR3	**0.80**	0.07	0.04	0.03	0.14	0.32	0.09	0.09	0.14	0.11	0.10	0.02
AWR5	**0.75**	0.09	-0.03	-0.08	0.19	0.36	0.11	0.17	0.17	0.09	0.03	0.09
AWR6	**0.71**	-0.01	0.14	0.11	0.03	0.40	-0.01	0.18	0.00	0.21	0.01	0.13
BEN1	0.02	**0.88**	-0.12	-0.14	0.22	0.02	0.12	-0.07	0.27	-0.06	-0.06	-0.02
BEN2	0.01	**0.86**	-0.13	-0.12	0.21	-0.02	0.20	-0.02	0.25	-0.04	0.01	0.02
BEN6	0.13	**0.78**	-0.02	-0.03	0.19	0.04	0.17	-0.02	0.22	0.02	0.09	0.00
BEN9	0.07	**0.75**	-0.05	-0.06	0.19	-0.03	0.19	-0.02	0.17	0.07	0.11	-0.03
CST1	0.04	0.04	**0.68**	0.17	-0.19	-0.03	-0.03	0.00	-0.11	0.12	0.09	0.00
CST2	0.03	-0.16	**0.92**	0.27	-0.34	-0.05	-0.14	0.06	-0.26	0.23	0.14	0.05
CST3	0.08	-0.09	**0.91**	0.25	-0.31	-0.02	-0.10	0.03	-0.23	0.22	0.20	0.04
DISP1	0.37	-0.02	-0.06	0.04	0.19	**0.86**	-0.03	0.34	0.02	0.22	-0.22	0.29
DISP2	0.32	0.11	-0.05	-0.07	0.24	**0.68**	0.14	0.22	0.20	0.15	-0.13	0.15
DISP3	0.44	-0.05	0.01	0.09	0.14	**0.87**	-0.01	0.32	-0.02	0.27	-0.17	0.24
MAL1	0.03	-0.12	0.22	**0.85**	-0.09	0.07	-0.25	0.35	-0.31	0.32	-0.11	0.36
MAL2	0.03	-0.12	0.25	**0.77**	-0.16	-0.02	-0.21	0.23	-0.23	0.23	0.01	0.30
MAL3	0.03	-0.04	0.23	**0.83**	-0.11	0.03	-0.30	0.34	-0.28	0.26	-0.12	0.34
PB5	0.21	0.19	-0.23	-0.03	**0.81**	0.23	0.21	0.17	0.35	0.03	-0.03	0.07
PB7	0.11	0.20	-0.26	-0.06	**0.82**	0.16	0.22	0.17	0.31	0.01	-0.10	0.04
PB_6	0.11	0.19	-0.31	-0.25	**0.72**	0.13	0.22	-0.02	0.32	-0.11	-0.13	-0.04
RE1	0.06	0.16	-0.13	-0.22	0.19	0.03	**0.84**	-0.19	0.45	-0.07	0.25	-0.21
RE2	0.06	0.13	-0.05	-0.26	0.20	0.02	**0.85**	-0.17	0.43	-0.03	0.26	-0.28
RE3	0.14	0.22	-0.11	-0.30	0.30	0.03	**0.86**	-0.10	0.51	-0.05	0.21	-0.17
RISK1	0.17	0.05	-0.03	0.23	0.16	0.32	-0.05	**0.72**	0.03	0.30	-0.23	0.44
RISK3	0.12	-0.09	0.07	0.33	0.10	0.25	-0.14	**0.73**	-0.13	0.42	-0.17	0.51
RISK4	0.16	-0.07	0.10	0.32	0.02	0.27	-0.15	**0.73**	-0.07	0.49	-0.23	0.51
RISK6	0.14	-0.02	0.01	0.29	0.08	0.30	-0.15	**0.80**	-0.06	0.48	-0.29	0.51
RISK7	0.15	-0.02	-0.03	0.28	0.15	0.29	-0.11	**0.79**	-0.06	0.40	-0.27	0.45
RISK8	0.17	-0.02	0.03	0.24	0.12	0.25	-0.16	**0.71**	-0.06	0.40	-0.25	0.50
SE1	0.11	0.23	-0.19	-0.28	0.35	0.04	0.47	-0.06	**0.84**	-0.13	0.07	-0.14
SE2	0.11	0.24	-0.23	-0.24	0.38	0.02	0.37	0.00	**0.80**	-0.15	-0.03	-0.03
SE3	0.08	0.25	-0.21	-0.34	0.31	0.08	0.51	-0.15	**0.82**	-0.19	0.21	-0.17
SE4	0.18	0.19	-0.16	-0.22	0.29	0.07	0.42	-0.05	**0.73**	-0.18	0.10	-0.06
SEV1	0.17	0.02	0.12	0.24	0.07	0.27	0.00	0.54	-0.09	**0.84**	-0.08	0.45
SEV2	0.13	0.00	0.25	0.30	-0.07	0.21	-0.11	0.44	-0.19	**0.85**	-0.03	0.38
SEV3	0.15	-0.05	0.24	0.32	-0.09	0.18	-0.06	0.40	-0.25	**0.81**	0.01	0.33
TRST1	0.05	-0.04	0.16	-0.07	-0.10	-0.20	0.20	-0.29	0.05	-0.01	**0.89**	-0.26
TRST2	0.05	0.11	0.15	-0.11	-0.10	-0.18	0.30	-0.27	0.15	-0.08	**0.86**	-0.30
VUL1	0.10	-0.02	0.02	0.24	0.09	0.27	-0.14	0.53	-0.11	0.41	-0.29	**0.77**
VUL2	0.14	0.00	0.06	0.31	0.06	0.23	-0.16	0.56	-0.07	0.43	-0.20	**0.79**
VUL3	0.09	0.06	-0.01	0.34	0.03	0.18	-0.26	0.45	-0.09	0.30	-0.31	**0.79**
VUL4	0.01	-0.07	0.05	0.39	-0.09	0.20	-0.25	0.49	-0.12	0.33	-0.22	**0.79**

APPENDIX C: Spearmean's Correlations Study 1

SPEARMEAN'S CORRELATIONS													
		AWARE	BENEFIT	COST	MAL	PB	DISP	RE	RISK	SE	SEV	TRUST	VUL
RE1	Correlation Coefficient	0.069	.169**	-.148**	-.213**	.216**	0.045	**.813****	-.159**	.475**	-0.073	.225**	-.190**
	Sig. (2-tailed)	0.158	0.001	0.003	0	0	0.361	**0**	0.001	0	0.138	0	0
RE2	Correlation Coefficient	0.074	.144**	-.109*	-.249**	.234**	0.051	**.859****	-.135**	.435**	-0.048	.232**	-.251**
	Sig. (2-tailed)	0.131	0.003	0.026	0	0	0.299	**0**	0.006	0	0.326	0	0
RE3	Correlation Coefficient	.162**	.253**	-.166**	-.279**	.334**	0.034	**.823****	-0.064	.524**	-0.04	.146**	-.151**
	Sig. (2-tailed)	0.001	0	0.001	0	0	0.495	**0**	0.192	0	0.421	0.003	0.002
SE1	Correlation Coefficient	.113*	.246**	-.269**	-.266**	.414**	0.042	.491**	-0.049	**.794****	-.141**	0.02	-.153**
	Sig. (2-tailed)	0.022	0	0	0	0	0.397	0	0.317	**0**	0.004	0.687	0.002
SE2	Correlation Coefficient	.147**	.239**	-.333**	-.246**	.418**	0.04	.404**	0.019	**.799****	-.157**	-0.039	-0.016
	Sig. (2-tailed)	0.003	0	0	0	0	0.414	0	0.693	**0**	0.001	0.425	0.748
SE3	Correlation Coefficient	.116*	.258**	-.272**	-.345**	.382**	.105*	.542**	-.099*	**.816****	-.197**	.151**	-.150**
	Sig. (2-tailed)	0.017	0	0	0	0	0.033	0	0.043	**0**	0	0.002	0.002
SE4	Correlation Coefficient	.181**	.189**	-.213**	-.227**	.353**	0.08	.433**	-0.015	**.738****	-.188**	0.059	-0.051
	Sig. (2-tailed)	0	0	0	0	0	0.105	0	0.755	**0**	0	0.229	0.303
CST1	Correlation Coefficient	0.013	0.03	**.703****	.180**	-.196**	-0.04	-0.072	0.018	-.151**	.126*	0.091	0.036
	Sig. (2-tailed)	0.786	0.538	**0**	0	0	0.419	0.145	0.711	0.002	0.01	0.064	0.465
CST2	Correlation Coefficient	-0.009	-.162**	**.898****	.289**	-.369**	-0.069	-.169**	0.061	-.307**	.217**	.120*	0.062
	Sig. (2-tailed)	0.849	0.001	**0**	0	0	0.162	0.001	0.212	0	0	0.014	0.207
CST3	Correlation Coefficient	0.046	-.108*	**.890****	.260**	-.334**	-0.032	-.133**	0.021	-.302**	.199**	.166**	0.056
	Sig. (2-tailed)	0.345	0.028	**0**	0	0	0.51	0.007	0.665	0	0	0.001	0.25
MAL1	Correlation Coefficient	0.023	-.135**	.241**	**.840****	-.128**	0.072	-.236**	.322**	-.297**	.318**	-0.089	.332**
	Sig. (2-tailed)	0.645	0.006	0	**0**	0.009	0.143	0	0	0	0	0.07	0
MAL2	Correlation Coefficient	0.016	-.105*	.272**	**.751****	-.192**	-0.005	-.189**	.206**	-.209**	.236**	0.03	.281**
	Sig. (2-tailed)	0.752	0.033	0	**0**	0	0.918	0	0	0	0	0.547	0
MAL3	Correlation Coefficient	0.033	-0.049	.230**	**.849****	-.149**	0.02	-.287**	.322**	-.281**	.262**	-0.078	.324**
	Sig. (2-tailed)	0.5	0.321	0	**0**	0.002	0.68	0	0	0	0	0.114	0
PB7	Correlation Coefficient	.102*	.237**	-.317**	-0.076	**.800****	.151**	.241**	.196**	.378**	0.007	-.152**	0.067
	Sig. (2-tailed)	0.037	0	0	0.12	**0**	0.002	0	0	0	0.884	0.002	0.172
PB6	Correlation Coefficient	.148**	.188**	-.348**	-.254**	**.741****	.151**	.254**	0.036	.363**	-.111*	-.148**	-0.012
	Sig. (2-tailed)	0.003	0	0	0	**0**	0.002	0	0.465	0	0.023	0.002	0.805
PB5	Correlation Coefficient	.205**	.233**	-.290**	-0.083	**.818****	.228**	.249**	.171**	.391**	0.002	-0.045	0.075
	Sig. (2-tailed)	0	0	0	0.092	**0**	0	0	0	0	0.974	0.359	0.126
RISK1	Correlation Coefficient	.157**	0.061	-0.041	.219**	.160**	.290**	0	**.678****	0.038	.278**	-.248**	.414**
	Sig. (2-tailed)	0.001	0.215	0.41	0	0.001	0	0.993	**0**	0.441	0	0	0
RISK3	Correlation Coefficient	.107*	-0.061	0.079	.327**	0.085	.233**	-.131**	**.714****	-.110*	.395**	-.175**	.487**
	Sig. (2-tailed)	0.029	0.215	0.106	0	0.082	0	0.007	**0**	0.025	0	0	0
RISK4	Correlation Coefficient	.161**	-0.075	.115*	.300**	-0.006	.249**	-.126*	**.720****	-0.07	.460**	-.207**	.484**
	Sig. (2-tailed)	0.001	0.126	0.019	0	0.91	0	0.01	**0**	0.155	0	0	0
RISK6	Correlation Coefficient	.137**	0.004	0.016	.263**	.101*	.282**	-.112*	**.775****	-0.034	.437**	-.277**	.450**
	Sig. (2-tailed)	0.005	0.927	0.743	0	0.039	0	0.022	**0**	0.486	0	0	0

RISK7	Correlation Coefficient	.136**	-0.02	-0.041	.261**	.171**	.271**	-0.059	**.762****	-0.031	.360**	-.269**	.411**
	Sig. (2-tailed)	0.005	0.687	0.406	0	0	0	0.228	**0**	0.527	0	0	0
RISK8	Correlation Coefficient	.186**	-0.013	0.02	.214**	.156**	.238**	-.118*	**.670****	-0.03	.356**	-.255**	.473**
	Sig. (2-tailed)	0	0.793	0.681	0	0.001	0	0.016	**0**	0.539	0	0	0
VUL1	Correlation Coefficient	0.093	-0.038	0.043	.241**	.116*	.248**	-.168**	.527**	-.104*	.395**	-.289**	**.762****
	Sig. (2-tailed)	0.057	0.445	0.379	0	0.018	0	0.001	0	0.033	0	0	**0**
VUL2	Correlation Coefficient	.163**	-0.012	0.072	.299**	0.049	.230**	-.144**	.533**	-0.074	.413**	-.189**	**.803****
	Sig. (2-tailed)	0.001	0.804	0.145	0	0.32	0	0.003	0	0.131	0	0	**0**
VUL3	Correlation Coefficient	.099*	0.078	-0.019	.314**	0.071	.183**	-.242**	.437**	-0.088	.271**	-.302**	**.743****
	Sig. (2-tailed)	0.044	0.112	0.696	0	0.148	0	0	0	0.072	0	0	**0**
VUL4	Correlation Coefficient	0.031	-0.067	0.036	.357**	-0.066	.231**	-.218**	.499**	-.110*	.313**	-.214**	**.769****
	Sig. (2-tailed)	0.525	0.172	0.46	0	0.176	0	0	0	0.025	0	0	**0**
SEV1	Correlation Coefficient	.170**	0.009	.097*	.236**	0.057	.238**	0.028	.522**	-0.092	**.833****	-0.086	.424**
	Sig. (2-tailed)	0	0.855	0.048	0	0.248	0	0.565	0	0.061	**0**	0.08	0
SEV2	Correlation Coefficient	.123*	0	.245**	.303**	-.104*	.181**	-.103*	.407**	-.200**	**.841****	-0.008	.369**
	Sig. (2-tailed)	0.012	0.995	0	0	0.033	0	0.036	0	0	**0**	0.876	0
SEV3	Correlation Coefficient	.145**	-0.066	.244**	.316**	-.135**	.154**	-0.08	.353**	-.256**	**.791****	0.056	.312**
	Sig. (2-tailed)	0.003	0.182	0	0	0.006	0.002	0.102	0	0	**0**	0.258	0
BEN1	Correlation Coefficient	0.023	**.856****	-.126*	-.122*	.266**	0.048	.140**	-0.017	.273**	-0.05	-.102*	0.014
	Sig. (2-tailed)	0.64	**0**	0.01	0.013	0	0.332	0.004	0.734	0	0.307	0.037	0.78
BEN2	Correlation Coefficient	-0.006	**.860****	-.142**	-.129**	.252**	0.01	.201**	-0.027	.310**	-0.072	-0.054	-0.001
	Sig. (2-tailed)	0.91	**0**	0.004	0.009	0	0.845	0	0.589	0	0.143	0.276	0.986
BEN6	Correlation Coefficient	.142**	**.789****	-0.05	-0.046	.244**	0.077	.201**	0.013	.252**	0.003	0.041	0.035
	Sig. (2-tailed)	0.004	**0**	0.304	0.354	0	0.116	0	0.785	0	0.948	0.405	0.472
BEN9	Correlation Coefficient	0.071	**.770****	-0.086	-0.092	.230**	-0.016	.216**	-0.014	.228**	0.024	0.071	-0.032
	Sig. (2-tailed)	0.146	**0**	0.078	0.062	0	0.749	0	0.783	0	0.618	0.148	0.514
AWR2	Correlation Coefficient	**.806****	0.061	0.02	0.058	.225**	.337**	.162**	.178**	.159**	.137**	0.04	.118*
	Sig. (2-tailed)	**0**	0.211	0.677	0.238	0	0	0.001	0	0.001	0.005	0.415	0.016
AWR3	Correlation Coefficient	**.762****	0.092	0.023	0.018	.155**	.333**	.127**	0.092	.168**	.108*	0.086	0.039
	Sig. (2-tailed)	**0**	0.06	0.647	0.717	0.002	0	0.01	0.061	0.001	0.028	0.08	0.428
AWR5	Correlation Coefficient	**.714****	.096*	-0.049	-.100*	.226**	.389**	.148**	.184**	.208**	0.075	0.02	0.087
	Sig. (2-tailed)	**0**	0.049	0.318	0.042	0	0	0.003	0	0	0.127	0.686	0.076
AWR6	Correlation Coefficient	**.736****	-0.008	.117*	.126**	0.039	.366**	-0.018	.167**	0.001	.193**	-0.004	.118*
	Sig. (2-tailed)	**0**	0.876	0.017	0.01	0.424	0	0.719	0.001	0.989	0	0.939	0.016
TRST1	Correlation Coefficient	0.051	-0.042	.149**	-0.054	-.136**	-.169**	.160**	-.298**	0.001	-0.001	**.935****	-.258**
	Sig. (2-tailed)	0.297	0.396	0.002	0.271	0.005	0.001	0.001	0	0.977	0.978	**0**	0
TRST2	Correlation Coefficient	0.052	0.078	.120*	-0.089	-0.09	-.153**	.270**	-.245**	.127**	-0.089	**.767****	-.298**
	Sig. (2-tailed)	0.292	0.113	0.014	0.068	0.067	0.002	0	0	0.01	0.071	**0**	0
DISP1	Correlation Coefficient	.382**	0.002	-0.079	0.029	.219**	**.848****	0.003	.335**	0.065	.192**	-.194**	.275**
	Sig. (2-tailed)	0	0.964	0.109	0.56	0	**0**	0.954	0	0.188	0	0	0
DISP2	Correlation Coefficient	.332**	.124*	-0.072	-0.061	.267**	**.639****	.164**	.238**	.204**	.146**	-.157**	.172**
	Sig. (2-tailed)	0	0.012	0.142	0.216	0	**0**	0.001	0	0	0.003	0.001	0
DISP3	Correlation Coefficient	.421**	-0.03	0.003	0.079	.138**	**.866****	0.033	.290**	0.024	.252**	-.131**	.240**
	Sig. (2-tailed)	0	0.548	0.958	0.107	0.005	**0**	0.507	0	0.623	0	0.008	0

**. Correlation is significant at the 0.01 level (2-tailed)

*. Correlation is significant at the 0.05 level (2-tailed).

APPENDIX D: Pearson's Correlations Study 1

PEARSON'S CORRELATIONS													
		AWARE	BENEFIT	COST	MAL	PB	DISP	RE	RISK	SE	SEV	TRUST	VUL
RE1	Pearson Correlation	0.059	.162**	-.127**	-.218**	.190**	0.028	**.836****	-.187**	.447**	-0.07	.254**	-.214**
	Sig. (2-tailed)	0.229	0.001	0.01	0	0	0.574	**0**	0	0	0.151	0	0
RE2	Pearson Correlation	0.056	.128**	-0.055	-.260**	.200**	0.021	**.853****	-.171**	.431**	-0.032	.265**	-.279**
	Sig. (2-tailed)	0.25	0.009	0.264	0	0	0.665	**0**	0	0	0.51	0	0
RE3	Pearson Correlation	.142**	.218**	-.110*	-.302**	.302**	0.027	**.865****	-.100*	.513**	-0.048	.212**	-.170**
	Sig. (2-tailed)	0.004	0	0.025	0	0	0.579	**0**	0.041	0	0.33	0	0
SE1	Pearson Correlation	.112*	.227**	-.188**	-.275**	.353**	0.045	.472**	-0.058	**.835****	-.129**	0.071	-.137**
	Sig. (2-tailed)	0.022	0	0	0	0	0.361	0	0.235	**0**	0.009	0.148	0.005
SE2	Pearson Correlation	.110*	.240**	-.234**	-.243**	.378**	0.015	.367**	-0.001	**.803****	-.150**	-0.035	-0.029
	Sig. (2-tailed)	0.025	0	0	0	0	0.758	0	0.984	**0**	0.002	0.479	0.562
SE3	Pearson Correlation	0.084	.249**	-.212**	-.337**	.310**	0.079	.505**	-.146**	**.825****	-.195**	.211**	-.174**
	Sig. (2-tailed)	0.087	0	0	0	0	0.11	0	0.003	**0**	0	0	0
SE4	Pearson Correlation	.177**	.187**	-.156**	-.220**	.287**	0.073	.415**	-0.052	**.734****	-.177**	.101*	-0.057
	Sig. (2-tailed)	0	0	0.001	0	0	0.139	0	0.286	**0**	0	0.039	0.245
CST1	Pearson Correlation	0.036	0.041	**.680****	.171**	-.185**	-0.027	-0.034	0.001	-.114*	.122*	0.086	0.003
	Sig. (2-tailed)	0.467	0.403	**0**	0	0	0.586	0.488	0.978	0.02	0.013	0.08	0.945
CST2	Pearson Correlation	0.028	-.159**	**.917****	.274**	-.340**	-0.05	-.136**	0.058	-.258**	.230**	.142**	0.054
	Sig. (2-tailed)	0.572	0.001	**0**	0	0	0.314	0.005	0.238	0	0	0.004	0.271
CST3	Pearson Correlation	0.077	-0.089	**.909****	.252**	-.307**	-0.023	-.096*	0.025	-.228**	.217**	.202**	0.035
	Sig. (2-tailed)	0.117	0.071	**0**	0	0	0.643	0.049	0.609	0	0	0	0.475
MAL1	Pearson Correlation	0.03	-.123*	.220**	**.854****	-0.087	0.069	-.252**	.346**	-.312**	.322**	-.114*	.363**
	Sig. (2-tailed)	0.538	0.012	0	**0**	0.078	0.162	0	0	0	0	0.02	0
MAL2	Pearson Correlation	0.033	-.121*	.250**	**.767****	-.163**	-0.018	-.209**	.231**	-.233**	.230**	0.011	.296**
	Sig. (2-tailed)	0.507	0.013	0	**0**	0.001	0.715	0	0	0	0	0.829	0
MAL3	Pearson Correlation	0.033	-0.043	.227**	**.831****	-.111*	0.029	-.297**	.336**	-.279**	.262**	-.121*	.336**
	Sig. (2-tailed)	0.505	0.383	0	**0**	0.023	0.552	0	0	0	0	0.013	0
PB7	Pearson Correlation	.114*	.199**	-.260**	-0.058	**.818****	.158**	.223**	.173**	.313**	0.013	-.104*	0.041
	Sig. (2-tailed)	0.02	0	0	0.235	**0**	0.001	0	0	0	0.795	0.035	0.41
PB6	Pearson Correlation	.111*	.187**	-.311**	-.255**	**.724****	.134**	.222**	-0.023	.318**	-.111*	-.135**	-0.042
	Sig. (2-tailed)	0.023	0	0	0	**0**	0.006	0	0.638	0	0.024	0.006	0.398
PB5	Pearson Correlation	.209**	.193**	-.233**	-0.034	**.807****	.232**	.215**	.167**	.348**	0.033	-0.027	0.072
	Sig. (2-tailed)	0	0	0	0.49	**0**	0	0	0.001	0	0.508	0.586	0.141
RISK1	Pearson Correlation	.167**	0.052	-0.027	.226**	.160**	.320**	-0.046	**.719****	0.026	.297**	-.235**	.439**
	Sig. (2-tailed)	0.001	0.293	0.587	0	0.001	0	0.35	**0**	0.599	0	0	0
RISK3	Pearson Correlation	.124*	-0.088	0.072	.326**	.105*	.247**	-.145**	**.730****	-.129**	.422**	-.169**	.508**
	Sig. (2-tailed)	0.011	0.074	0.143	0	0.033	0	0.003	**0**	0.008	0	0.001	0
RISK4	Pearson Correlation	.159**	-0.07	.104*	.320**	0.024	.274**	-.147**	**.734****	-0.071	.495**	-.231**	.512**
	Sig. (2-tailed)	0.001	0.152	0.034	0	0.631	0	0.003	**0**	0.151	0	0	0
RISK6	Pearson Correlation	.143**	-0.024	0.011	.287**	0.076	.299**	-.149**	**.801****	-0.063	.475**	-.287**	.506**
	Sig. (2-tailed)	0.003	0.631	0.819	0	0.122	0	0.002	**0**	0.197	0	0	0

RISK7	Pearson Correlation	.145**	-0.019	-0.029	.278**	.155**	.287**	-.110*	**.787****	-0.06	.399**	-.268**	.452**
	Sig. (2-tailed)	0.003	0 . 7	0.555	0	0.002	0	0.025	**0**	0.224	0	0	0
RISK8	Pearson Correlation	.167**	-0.019	0.027	.245**	.121*	.253**	-.163**	**.713****	-0.055	.400**	-.251**	.501**
	Sig. (2-tailed)	0.001	0.694	0.581	0	0.013	0	0.001	**0**	0.263	0	0	0
VUL1	Pearson Correlation	.104*	-0.021	0.022	.240**	0.091	.269**	-.140**	.525**	-.112*	.405**	-.295**	**.768****
	Sig. (2-tailed)	0.034	0.676	0.652	0	0.065	0	0.004	0	0.022	0	0	**0**
VUL2	Pearson Correlation	.144**	0.001	0.059	.314**	0.057	.229**	-.162**	.563**	-0.071	.426**	-.197**	**.791****
	Sig. (2-tailed)	0.003	0.989	0.229	0	0.25	0	0.001	0	0.149	0	0	**0**
VUL3	Pearson Correlation	0.093	0.064	-0.005	.343**	0.035	.179**	-.257**	.450**	-0.094	.301**	-.307**	**.786****
	Sig. (2-tailed)	0.059	0.196	0.913	0	0.479	0	0	0	0.054	0	0	**0**
VUL4	Pearson Correlation	0.013	-0.065	0.047	.386**	-0.088	.204**	-.251**	.491**	-.122*	.328**	-.219**	**.789****
	Sig. (2-tailed)	0.792	0.183	0.34	0	0.073	0	0	0	0.013	0	0	**0**
SEV1	Pearson Correlation	.170**	0.019	.119*	.237**	0.068	.272**	0.005	.542**	-0.087	**.840****	-0.084	.447**
	Sig. (2-tailed)	0	0.702	0.015	0	0.168	0	0.922	0	0.077	**0**	0.089	0
SEV2	Pearson Correlation	.129**	0	.246**	.297**	-0.069	.211**	-.106*	.438**	-.194**	**.846****	-0.029	.380**
	Sig. (2-tailed)	0.008	0.993	0	0	0.158	0	0.03	0	0	**0**	0.555	0
SEV3	Pearson Correlation	.155**	-0.053	.239**	.315**	-0.088	.176**	-0.056	.397**	-.252**	**.812****	0.013	.335**
	Sig. (2-tailed)	0.002	0.277	0	0	0.074	0	0.251	0	0	**0**	0.789	0
BEN1	Pearson Correlation	0.019	**.883****	-.116*	-.144**	.218**	0.024	.120*	-0.066	.270**	-0.062	-0.062	-0.021
	Sig. (2-tailed)	0.704	**0**	0.017	0.003	0	0.625	0.015	0.179	0	0.205	0.207	0.664
BEN2	Pearson Correlation	0.006	**.858****	-.126**	-.118*	.208**	-0.015	.202**	-0.02	.254**	-0.042	0.005	0.017
	Sig. (2-tailed)	0.901	**0**	0.01	0.016	0	0.756	0	0.689	0	0.398	0.913	0.729
BEN6	Pearson Correlation	.132**	**.779****	-0.019	-0.026	.193**	0.043	.175**	-0.023	.222**	0.024	0.092	0.005
	Sig. (2-tailed)	0.007	**0**	0.707	0.599	0	0.378	0	0.634	0	0.629	0.062	0.924
BEN9	Pearson Correlation	0.065	**.748****	-0.049	-0.065	.189**	-0.03	.186**	-0.017	.173**	0.073	.107*	-0.029
	Sig. (2-tailed)	0.186	**0**	0.316	0.188	0	0.546	0	0.724	0	0.137	0.029	0.556
AWR2	Pearson Correlation	**.832****	0.047	0.018	0.059	.222**	.355**	.148**	.166**	.153**	.144**	0.053	.107*
	Sig. (2-tailed)	**0**	0.338	0.707	0.233	0	0	0.002	0.001	0.002	0.003	0.277	0.03
AWR3	Pearson Correlation	**.801****	0.072	0.036	0.026	.141**	.321**	0.094	0.088	.141**	.105*	.096*	0.019
	Sig. (2-tailed)	**0**	0.14	0.468	0.592	0.004	0	0.056	0.072	0.004	0.032	0.05	0.697
AWR5	Pearson Correlation	**.750****	0.089	-0.035	-0.084	.191**	.364**	.113*	.170**	.171**	0.093	0.03	0.087
	Sig. (2-tailed)	**0**	0.07	0.482	0.086	0	0	0.021	0	0	0.059	0.538	0.075
AWR6	Pearson Correlation	**.710****	-0.013	.140**	.111*	0.031	.401**	-0.01	.184**	0.002	.211**	0.01	.131**
	Sig. (2-tailed)	**0**	0.784	0.004	0.024	0.525	0	0.837	0	0.963	0	0.84	0.008
TRST1	Pearson Correlation	0.048	-0.041	.155**	-0.066	-.098*	-.196**	.197**	-.295**	0.048	-0.005	**.888****	-.261**
	Sig. (2-tailed)	0.324	0.399	0.001	0.177	0.045	0	0	0	0.328	0.918	**0**	0
TRST2	Pearson Correlation	0.054	.106*	.151**	-.109*	-0.096	-.182**	.301**	-.266**	.146**	-0.079	**.861****	-.305**
	Sig. (2-tailed)	0.271	0.031	0.002	0.026	0.05	0	0	0	0.003	0.107	**0**	0
DISP1	Pearson Correlation	.366**	-0.019	-0.059	0.045	.186**	**.859****	-0.028	.343**	0.017	.222**	-.217**	.287**
	Sig. (2-tailed)	0	0.692	0.229	0.362	0	**0**	0.562	0	0.725	0	0	0
DISP2	Pearson Correlation	.319**	.110*	-0.054	-0.069	.237**	**.678****	.139**	.224**	.196**	.146**	-.128**	.148**
	Sig. (2-tailed)	0	0.024	0.275	0.161	0	**0**	0.004	0	0	0.003	0.009	0.002
DISP3	Pearson Correlation	.442**	-0.047	0.007	0.086	.139**	**.866****	-0.009	.324**	-0.017	.269**	-.172**	.237**
	Sig. (2-tailed)	0	0.341	0.894	0.081	0.004	**0**	0.85	0	0.731	0	0	0

**. Correlation is significant at the 0.01 level (2-tailed)
*. Correlation is significant at the 0.05 level (2-tailed).

APPENDIX E: Essay Manipulations

HIGH THREAT

Your personal information is more than your name, address and social security number. It includes your shopping habits, driving record, medical diagnoses, work history, credit score and much more. Unfortunately, personal privacy is lost, unknowingly forfeited, purchased or stolen every day, often while using the Internet. Lost privacy can also mean that your personal information is collected, analyzed and shared by others without your knowledge or consent. You may learn that your privacy has been breached only after you've been refused a job, denied a student loan or mortgage, or even been arrested.

Identity theft (ID theft) is a common consequence of a privacy breaches. ID theft occurs when someone uses your personally identifiable information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes. As many as 15 million Americans have their identities stolen every year. This occurs so often that approximately every 3 seconds an identity is stolen! The financial losses resulting from ID theft are $50 billion or $3,500 per person. In fact, it is very likely that you or someone you know may have experienced some form of ID theft.

ID theft is very serious. The crime takes many forms. Identity thieves may rent an apartment, obtain a credit card, establish a telephone account in your name, or create a fake e-mail or Facebook account. You may not find out about the theft until after a negative consequence (for example, contacted by a debt collector for a loan someone else took out in your name). While some ID theft victims can resolve their problems quickly, others spend thousands of dollars and months repairing damage to their good name and credit record. This lost privacy can mean lost job opportunities, denial of loans (for education, housing, cars), and even arrest for crimes you did not commit. It can mean months or years of dealing with debt collectors, police, credit bureaus and government agencies. This loss of privacy can mean that no place is safe - because our 'electronic footprint' makes it very difficult to live and work without creating a record that can be traced by a web-savvy stalker.

LOW THREAT

Your personal information includes your name, address, social security number, shopping habits, driving record, medical diagnoses, work history, and credit score among others. While using the Internet it is possible for this information to be accessed without your consent. One form of privacy breach is Identity theft (ID theft). This occurs when someone uses your personally identifying information, without your permission. However, only a small minority (about 3%) of Americans experience some form of ID theft and of these people 75% recover their losses by reporting the incident to the police, credit card agencies or banks.

HIGH EFFICACY

ID theft occurs primarily because of the following two reasons:

- Poor computer security protection by individuals, and/or
- Poor computer security protection measures used by companies with whom individuals interact (for example, banks, employer etc).

You can protect yourself effectively against ID theft by using the following **ID Protection measures:**

i) installing security protection software, and ii) checking your credit report.

Security Protection Software typically consists of at least the following three components: software firewall, anti-virus protection and spyware protection (for example, products from Norton, McAfee , AVG among others). This software is commonly available, (even free as in the case of AVG), easy to install and use. They protect your individual computers from malicious software such as viruses and spyware. The security software automatically detects and removes existing installations of these malicious programs from your computer and guards against future intrusions.

Check your credit report for free annually through the government mandated web site – annualcreditreport.com – which provides your credit report from three credit reporting agencies (Experian, Equifax and Transunion). This check helps you ensure that your information residing

on other companies' databases have not been stolen and misused. This step you take is very effective (please note that this does not effect your credit score in any way as it is intended for your protection) in protecting your identity due to others' mistakes.

These two ID protection measures steps are easy to do and are extremely effective at protecting your information and guarding you from ID theft.

LOW EFFICACY

ID theft occurs primarily because of the following two reasons:

- Poor computer security protection by individuals, or
- Poor computer security protection measures used by companies with whom individuals interact (for example, banks, employer etc).

You can **attempt** to protect yourself against ID theft by installing security protection software, and checking your credit report. However, these are both imperfect solutions.

You can install home security software. However, **there is no such thing as 100% computer security**. Even when you use security software, your computer system can be breached since hackers target security software loopholes and use them to gain entry to your computer.

Even if you are careful about whom you disclose your information to, your private information can be misused by websites or companies that you shared your information with willingly, and you have no control over this because you are relying on the security of other organizations. As mentioned earlier, there is no such thing as 100% computer security and it is possible for your data to be stolen from these companies (even unintentionally). In addition, websites often make changes to their service and privacy policies without notifying users of the changes and of their consequences.

You can check your credit report. However, checking your credit report also will only tell you if you have had a breach already (after the occurrence of the negative event). But, it will not help protect you from the breach in the first place.

Therefore, these ID protection measures are NOT fully effective in guarding against ID theft.

APPENDIX F: Instrument Study 2

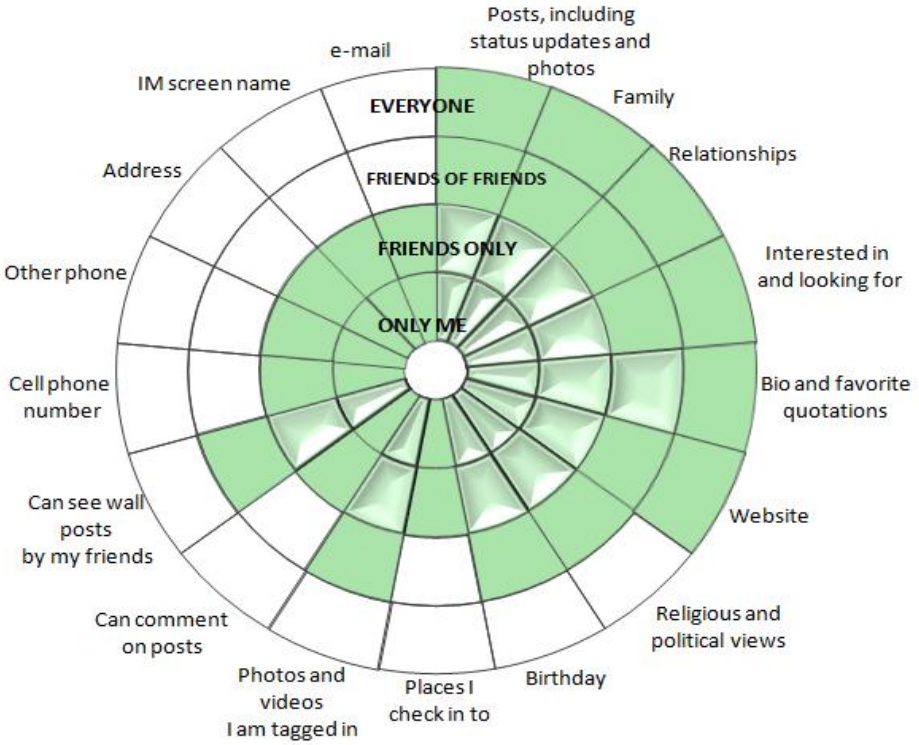
	VULNERABILITY (Witte 1996)
VUL1	I am at risk for identity theft
VUL2	It is highly likely that my identity will be stolen
VUL3	It is possible that my identity will be stolen
	SEVERITY (Witte 1996 items 1-3, Meservy 2010 items 4-5)
SEV1	If my identity were stolen it would have serious negative consequences for me
SEV2	If my identity were stolen it would have severe negative consequences for me
SEV3	If my identity were stolen it would have significant negative consequences for me
SEV4	If my identity were stolen it would be damaging to me
SEV4	If my identity were stolen it would bother me.
	RESPONSE EFFICACY (Witte et al. 1996)
RE1a	Using security software (one of the ID Protection measures) works in preventing identity theft
RE2a	Using security software (one of the ID Protection measures) is effective in preventing identity theft
RE3a	If I use security software (one of ID Protection measures) I am less likely to have my identity stolen
RE1b	Performing a credit check (one of the ID Protection measures) works in preventing identity theft
RE2b	Performing a credit check (one of the ID Protection measures) is effective in preventing identity theft
RE3b	If I perform a credit check (one of the ID Protection measures) I am less likely to have my identity stolen
	SELF EFFICACY (Witte 1996 items 1-3, Armitage et al. 1999 item 4)
SE1a	Security software (one of the ID Protection measures) is easy to use
SE2a	Security software (one of the ID Protection measures) is convenient to use
SE3a	I am able to use security software (one of the ID Protection measures) without much effort
SE4a	I believe I have the ability to use security software (one of the ID Protection measures)
SE1b	A credit check (one of the ID Protection measures) is easy to do
SE2b	A credit check (one of the ID Protection measures) is convenient to do
SE3b	I am able to do a credit check (one of the ID Protection measures) without much effort
SE4b	I believe I have the ability to do a credit check (one of the ID Protection measures)

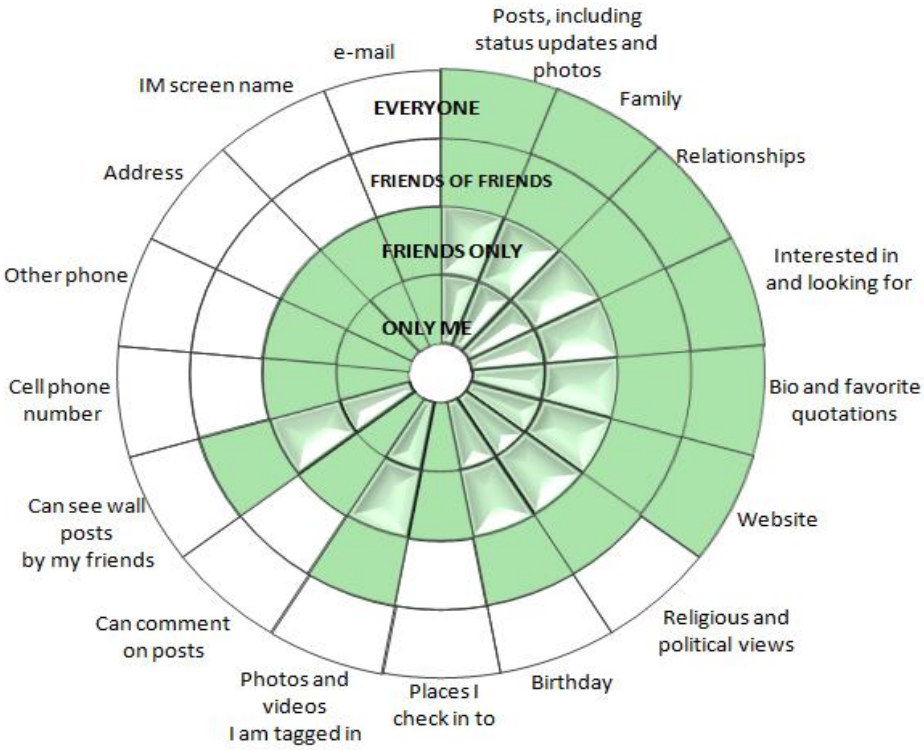
	THREAT (Liang and Xue 2010)
THRT1	Identity theft poses a threat to me
THRT2	The trouble caused by Identity theft threatens me
THRT3	Identity theft is a danger to me
THRT4	It is dreadful if my identity is stolen
	FEAR (Witte 1994, Dillard 2004)
FEAR1	I feel fearful when I think about identity theft
FEAR2	I feel worried when I think about identity theft
FEAR3	I feel nervous when I think about identity theft
FEAR4	I feel anxious when I think about identity theft
FEAR5	I feel scared when I think about identity theft
FEAR6	I feel afraid when I think about identity theft
DEPENDENT VARIABLES	
	MALADAPTIVE BEHAVIOR (Ho et al. 2005 items 1-3, Umeh et al. 2004 item 4)
MAL1	I do not need to engage in ID protection behaviors
MAL2	I am unlikely to experience identity theft, as I never had a problem in the past
MAL3*	Not experiencing identity theft is a matter of good luck
MAL4	I don't worry about ID theft because the chance of having my ID stolen is almost nonexistent
	BEHAVIORAL INTENTION
BISS1ID	I intend to use security software to protect my identity
BISS2ID	I predict I will security software to protect my identity
BISS3ID	I plan to use security software to protect my identity
BICC1ID	I intend to get a credit check to protect my identity
BICC2ID	I predict I will get a credit check to protect my identity
BICC3ID	I plan to get a credit check to protect my identity
*dropped item	

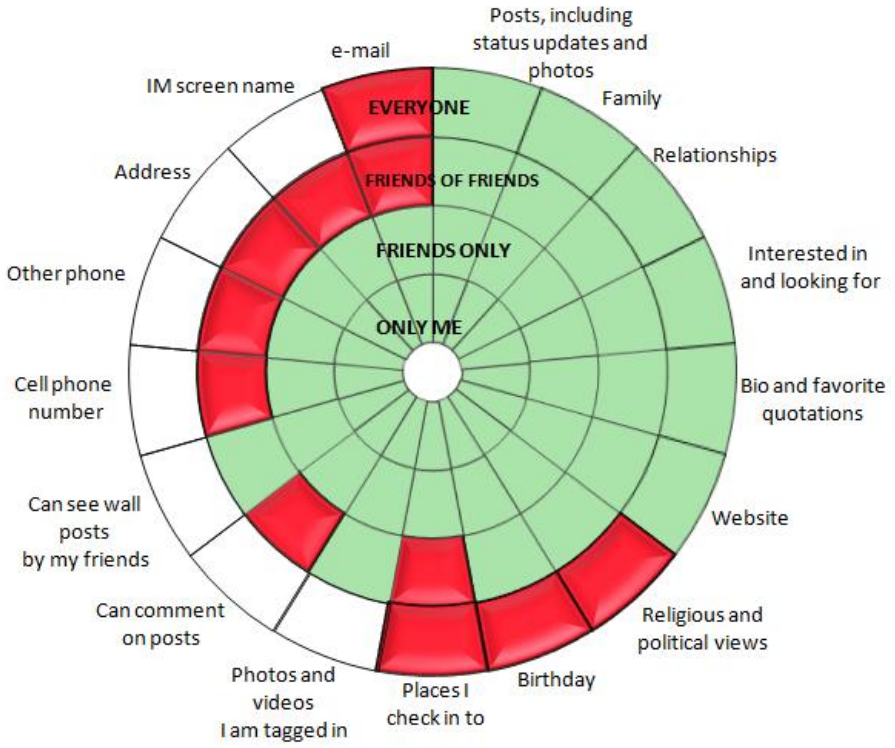
APPENDIX G: Instrument Study 3

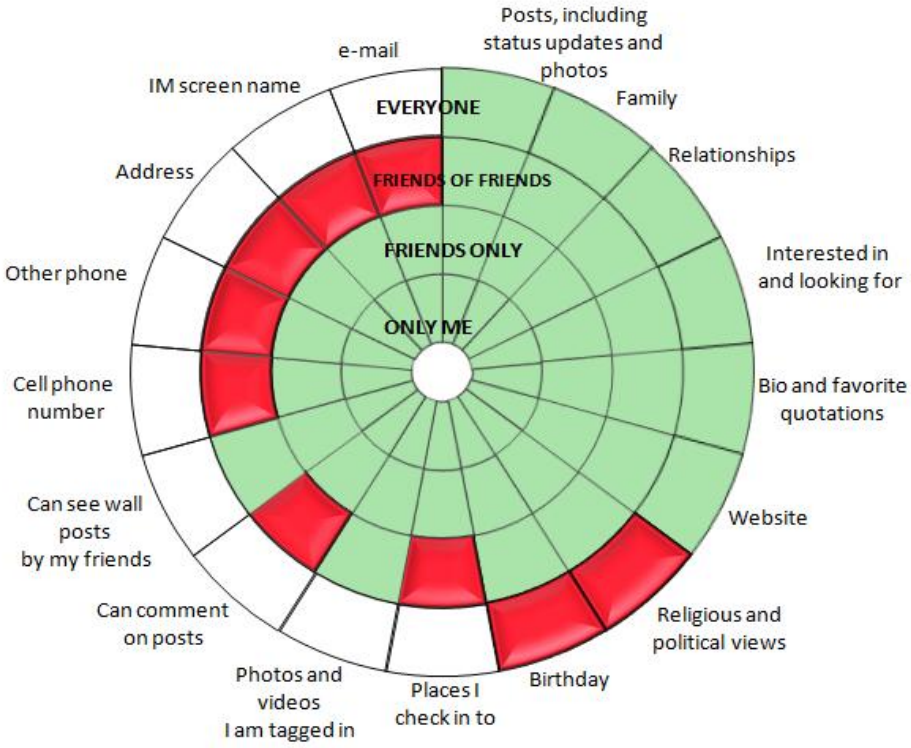
Questions for both wheel interface and table interface	
simple1	What is the user's setting for the "e-mail" category?
simple2	What is the user's setting for the "Bio and favorite quotations" category?
simple3	What is the user's setting for the "Can see wall posts by my friends" category?
simple4	What is the user's setting for the Can see wall posts by my friends category?
simple5	What is the user's setting for the "e-mail" category?
simple6	What is the user's setting for the "Cell phone number" category?
simple7	What is the default (recommended) setting for the "Website" category?
simple8	What is the user's setting for the "Website" category?
simple9	What is the default (recommended) setting for the "Can comment on posts category"?
complex1	Which setting(s) did this user set to "Friends only" , when the default (recommended) setting was "Everyone"?
complex2	Which setting(s) did this user set to "Friends of friends" only , when the default (recommended) setting was "Everyone"?
complex3	Compare the two charts above: Which of the two users left(A) or right (B) changed more settings?
complex4	Compare the two charts above: Which of the two users left (A) or right (B) has chosen 'safer' settings?
complex5	Compare the two charts above: Which of the two users left (A) or right (B) has chosen 'safer' settings?
complex6	Compare the two charts above: Which of the two users left (A) or right (B) has chosen 'safer' settings?
complex7	Which setting(s) did this user set differently than the default (recommended) setting?
complex8	Which setting(s) did this user set differently than the default (recommended) setting?
complex9	Which setting(s) did this user set to "Friends of friends", when the default (recommended) setting was "Friends Only"?
complex10	According to the default (recommended) setting which information is safe to disclose to "Friends Only"?
complex11	According to the default (recommended) setting, which information is safe to disclose to "Everyone"?

APPENDIX H: Interfaces Study 3






Posts, including status updates and photos
Family
Relationships
Interested in and looking for
Bio and favorite quotations
Website
Religious and political views
Birthday
Places I check in to
Photos and videos I am tagged in
Can comment on posts
Can see wall posts by my friends
Cell phone number
Other phone
Address
IM screen name
e-mail
EVERYONE
FRIENDS OF FRIENDS
FRIENDS ONLY
ONLY ME


Posts, including status updates and photos
Family
Relationships
Interested in and looking for
Bio and favorite quotations
Website
Religious and political views
Birthday
Places I check in to
Photos and videos I am tagged in
Can comment on posts
Can see wall posts by my friends
Cell phone number
Other phone
Address
IM screen name
e-mail
EVERYONE
FRIENDS OF FRIENDS
FRIENDS ONLY
ONLY ME

DEFAULT

	Everyone	Friends of Friends	Friends Only	Only Me
Posts, including status updates and photos	•			
Family	•			
Relationships	•			
Interested in and looking for	•			
Bio and favorite quotations	•			
Website	•			
Religious and political views		•		
Birthday		•		
Places I check in to			•	
Photos and videos I am tagged in		•		
Can comment on posts			•	
Can see wall posts by my friends		•		
Cell phone number			•	
Other phone			•	
Address			•	
IM screen name			•	
e-mail			•	

User B

	Everyone	Friends of Friends	Friends Only	Only Me
Posts, including status updates and photos			•	
Family			•	
Relationships			•	
Interested in and looking for			•	
Bio and favorite quotations			•	
Website			•	
Religious and political views			•	
Birthday			•	
Places I check in to			•	
Photos and videos I am tagged in			•	
Can comment on posts			•	
Can see wall posts by my friends			•	
Cell phone number			•	
Other phone			•	
Address			•	
IM screen name			•	
e-mail			•	

DEFAULT

	Everyone	Friends of Friends	Friends Only	Only Me
Posts, including status updates and photos	•			
Family	•			
Relationships	•			
Interested in and looking for	•			
Bio and favorite quotations	•			
Website	•			
Religious and political views		•		
Birthday		•		
Places I check in to			•	
Photos and videos I am tagged in		•		
Can comment on posts			•	
Can see wall posts by my friends		•		
Cell phone number			•	
Other phone			•	
Address			•	
IM screen name			•	
e-mail			•	

USER A

	Everyone	Friends of Friends	Friends Only	Only Me
Posts, including status updates and photos	•			
Family	•			
Relationships	•			
Interested in and looking for	•			
Bio and favorite quotations	•			
Website	•			
Religious and political views	•			
Birthday	•			
Places I check in to	•			
Photos and videos I am tagged in		•		
Can comment on posts		•		
Can see wall posts by my friends		•		
Cell phone number		•		
Other phone		•		
Address		•		
IM screen name		•		
e-mail	•			

DEFAULT

	Everyone	Friends of Friends	Friends Only	Only Me
Posts, including status updates and photos	•			
Family	•			
Relationships	•			
Interested in and looking for	•			
Bio and favorite quotations	•			
Website	•			
Religious and political views		•		
Birthday		•		
Places I check in to			•	
Photos and videos I am tagged in		•		
Can comment on posts			•	
Can see wall posts by my friends		•		
Cell phone number			•	
Other phone			•	
Address			•	
IM screen name			•	
e-mail			•	

USER A

	Everyone	Friends of Friends	Friends Only	Only Me
Posts, including status updates and photos			•	
Family			•	
Relationships			•	
Interested in and looking for			•	
Bio and favorite quotations		•		
Website			•	
Religious and political views			•	
Birthday			•	
Places I check in to			•	
Photos and videos I am tagged in			•	
Can comment on posts			•	
Can see wall posts by my friends			•	
Cell phone number			•	
Other phone			•	
Address			•	
IM screen name			•	
e-mail			•	

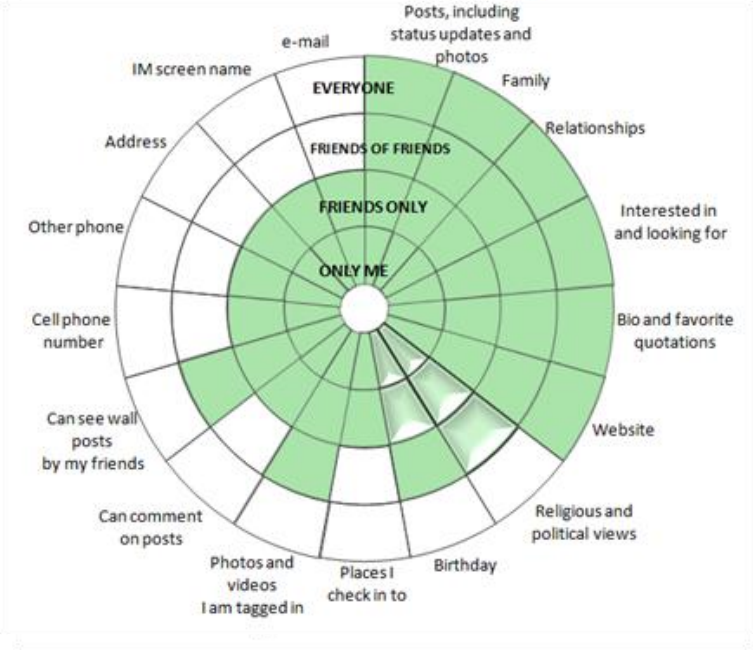
DEFAULT

	Everyone	Friends of Friends	Friends Only	Only Me
Posts, including status updates and photos	•			
Family	•			
Relationships	•			
Interested in and looking for	•			
Bio and favorite quotations	•			
Website	•			
Religious and political views		•		
Birthday		•		
Places I check in to			•	
Photos and videos I am tagged in		•		
Can comment on posts			•	
Can see wall posts by my friends		•		
Cell phone number			•	
Other phone			•	
Address			•	
IM screen name			•	
e-mail			•	

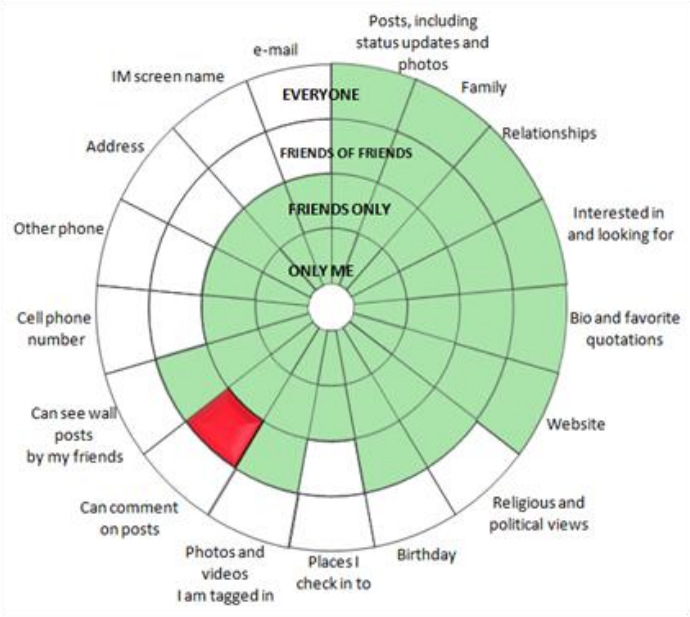
USER B

	Everyone	Friends of Friends	Friends Only	Only Me
Posts, including status updates and photos	•			
Family	•			
Relationships	•			
Interested in and looking for	•			
Bio and favorite quotations	•			
Website	•			
Religious and political views	•			
Birthday	•			
Places I check in to		•		
Photos and videos I am tagged in		•		
Can comment on posts		•		
Can see wall posts by my friends		•		
Cell phone number		•		
Other phone		•		
Address		•		
IM screen name		•		
e-mail		•		

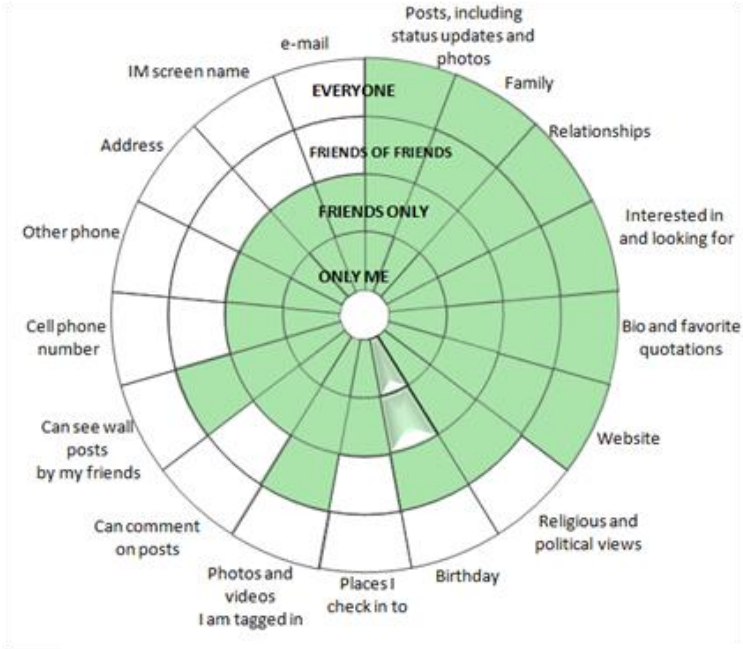
Comparison Images



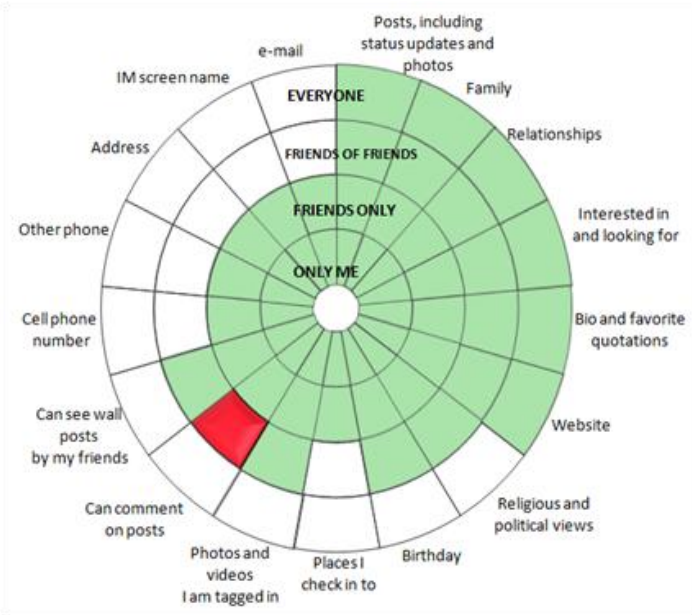
USER A (LEFT)



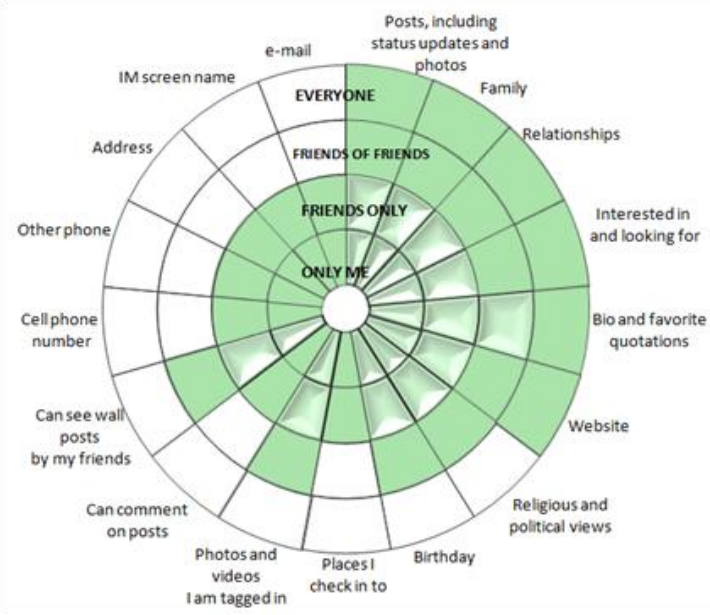
USER B (RIGHT)



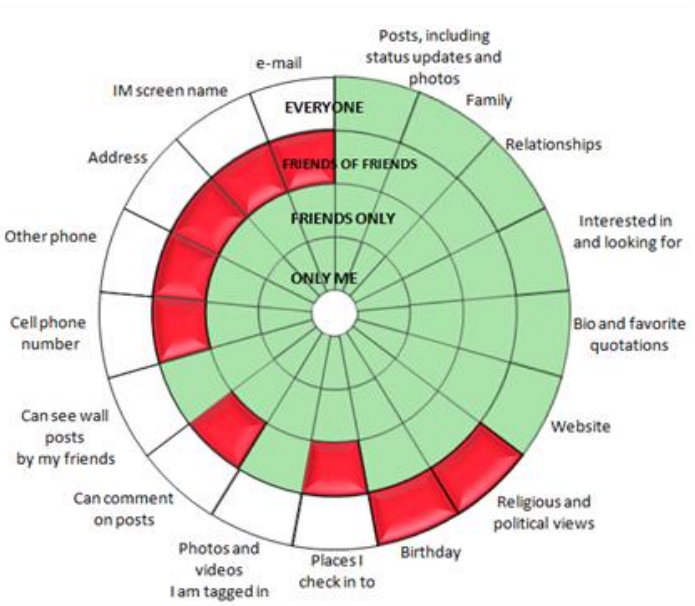
USER A (LEFT)



USER B (RIGHT)



USER A (LEFT)



USER B (RIGHT)

DEFAULT

	Everyone	Friends of Friends	Friends Only	Only Me
Posts, including status updates and photos	•			
Family	•			
Relationships	•			
Interested in and looking for	•			
Bio and favorite quotations	•			
Website	•			
Religious and political views		•		
Birthday		•		
Places I check in to			•	
Photos and videos I am tagged in		•		
Can comment on posts			•	
Can see wall posts by my friends		•		
Cell phone number			•	
Other phone			•	
Address			•	
IM screen name			•	
e-mail			•	

USER A (MIDDLE)

	Everyone	Friends of Friends	Friends Only	Only Me
Posts, including status updates and photos	•			
Family	•			
Relationships	•			
Interested in and looking for	•			
Bio and favorite quotations	•			
Website		•		
Religious and political views			•	
Birthday		•		
Places I check in to			•	
Photos and videos I am tagged in		•		
Can comment on posts			•	
Can see wall posts by my friends		•		
Cell phone number			•	
Other phone			•	
Address			•	
IM screen name			•	
e-mail			•	

USER B (RIGHT)

	Everyone	Friends of Friends	Friends Only	Only Me
Posts, including status updates and photos	•			
Family	•			
Relationships	•			
Interested in and looking for	•			
Bio and favorite quotations	•			
Website	•			
Religious and political views		•		
Birthday		•		
Places I check in to			•	
Photos and videos I am tagged in		•		
Can comment on posts		•		
Can see wall posts by my friends		•		
Cell phone number			•	
Other phone			•	
Address			•	
IM screen name			•	
e-mail			•	

DEFAULT

	Everyone	Friends of Friends	Friends Only	Only Me
Posts, including status updates and photos	•			
Family	•			
Relationships	•			
Interested in and looking for	•			
Bio and favorite quotations	•			
Website	•			
Religious and political views		•		
Birthday		•		
Places I check in to			•	
Photos and videos I am tagged in		•		
Can comment on posts			•	
Can see wall posts by my friends		•		
Cell phone number			•	
Other phone			•	
Address			•	
IM screen name			•	
e-mail			•	

USER A (MIDDLE)

	Everyone	Friends of Friends	Friends Only	Only Me
Posts, including status updates and photos			•	
Family			•	
Relationships			•	
Interested in and looking for			•	
Bio and favorite quotations		•		
Website			•	
Religious and political views			•	
Birthday			•	
Places I check in to			•	
Photos and videos I am tagged in			•	
Can comment on posts			•	
Can see wall posts by my friends			•	
Cell phone number			•	
Other phone			•	
Address			•	
IM screen name			•	
e-mail			•	

USER B (RIGHT)

	Everyone	Friends of Friends	Friends Only	Only Me
Posts, including status updates and photos	•			
Family	•			
Relationships	•			
Interested in and looking for	•			
Bio and favorite quotations	•			
Website	•			
Religious and political views	•			
Birthday	•			
Places I check in to		•		
Photos and videos I am tagged in		•		
Can comment on posts		•		
Can see wall posts by my friends		•		
Cell phone number		•		
Other phone		•		
Address		•		
IM screen name		•		
e-mail		•		

DEFAULT

	Everyone	Friends of Friends	Friends Only	Only Me
Posts, including status updates and photos	•			
Family	•			
Relationships	•			
Interested in and looking for	•			
Bio and favorite quotations	•			
Website	•			
Religious and political views		•		
Birthday		•		
Places I check in to			•	
Photos and videos I am tagged in		•		
Can comment on posts			•	
Can see wall posts by my friends		•		
Cell phone number			•	
Other phone			•	
Address			•	
IM screen name			•	
e-mail			•	

USER A (MIDDLE)

	Everyone	Friends of Friends	Friends Only	Only Me
Posts, including status updates and photos	•			
Family	•			
Relationships	•			
Interested in and looking for	•			
Bio and favorite quotations	•			
Website	•			
Religious and political views		•		
Birthday			•	
Places I check in to			•	
Photos and videos I am tagged in		•		
Can comment on posts			•	
Can see wall posts by my friends		•		
Cell phone number			•	
Other phone			•	
Address			•	
IM screen name			•	
e-mail			•	

USER B (RIGHT)

	Everyone	Friends of Friends	Friends Only	Only Me
Posts, including status updates and photos	•			
Family	•			
Relationships	•			
Interested in and looking for	•			
Bio and favorite quotations	•			
Website	•			
Religious and political views		•		
Birthday		•		
Places I check in to			•	
Photos and videos I am tagged in		•		
Can comment on posts			•	
Can see wall posts by my friends		•		
Cell phone number		•		
Other phone			•	
Address			•	
IM screen name			•	
e-mail			•	

REFERENCES

Acquisti, A. (2004). Privacy in Electronic Commerce and the Economics of Immediate Gratification, *Proceedings of ACM Electronic Commerce Conference*. New York, NY 21-29.

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook., *Proceedings of 6th Workshop on Privacy Enhancing Technologies.*

Acquisti, A., and Grossklags, J. (2004). "Privacy attitudes and privacy behavior" In Camp J. and Lewis, R. (Eds). *The Economics of Information security*. Kluwer.

Aiken, L. S., & West, S. G. (1991). *Multiple Regression: Testing and InterpretingInteractions*. Sage Publications, Beverly Hills, CA.

Aljifri, H., & Navarro, D.S. (2004). Search engines and privacy. *Computers and Security.* **23** (5) 379-388.

Altman, I. (1975). *The Environment and Social Behavior*. Brooks/Cole Publishing Company. Monterey CA

Anderson, P. & Dempsey, J. (2003). Privacy and E-Government: Privacy Impact Assessments and Privacy Commissioners. *Global Internet Policy Initiative.* Retrieved November 17, 2005 from http://www.internetpolicy.net/practices/030501pia.pdf.

Andrews, L., & Boyle, M. (2008). Consumers' accounts of perceived risk online and the influence of communication sources. *Qualitative Market Research, an International Journal.* **11** (1) 59-75.

Approach for measuring interaction effects: Results from a monte carlo simulation study And voice mail emotion/adoption study, *Proceedings Of The Seventeenth International Conference On Information Systems,* December 16-18, Cleveland, Ohio.

Arami, M., Treiblmaier, H., Pinterits, A., & Madleberger, M. (2004). Information privacy concerns and E-commerce: an empirical investigation. *Proceedings of the tenth Americas conference on information systems.* August 6-8, New York, New York.

Arthur, D., & Quester, P. (2004). Who's Afraid of That Ad? Applying Segmentation to the Protection Motivation Mode, *Psychology & Marketing*, **21** (9) 671

Bandura. A. (1977). Self-efficacy: Toward a unifying theory of behavioral Change. *Psychological Review.* **84** 191-215

Barclay, D., Thompson, R., & Higgins, C. (1995). The Partial Least Squares (PLS) Approach to Causal Modeling Persoanl Computer Adoption and Use an illustration, *Technology Studies* **2** (2) 285-309.

Barnes, J. (1954). Class and Committees in a Norwegian Island Parish. *Human Relations.* **7** (1) 39-58.

Barnes, S. (2006). A privacy paradox: Social networking in the United States. First Monday, 11 (9). Retrieved May 7, 2007 from http://www.firstmonday.org/issues/issue11_9/barnes/index.html

Bauer, Raymond A. (1967). Consumer behavior as risk taking. In Cox, D.F. (Ed). *Risk taking and information handling in consumer behavior.* Boston Graduate school of business administration Harvard University. 23-33.

Belanger, F. and Hiller, J.S. (2006). A framework for e-government: Privacy implications. *Business process management journal.* **12** (1) 48-60.

Belanger, F., & Carter, L. (2008). Trust and Risk in e-government adoption. *Journal of Strategic Information Systems* **17** 165-176.

Bellman, S., Johnson, E., Kobrin, S., & Lohse, G. (2004). International differences in information privacy concerns: a global survey of consumers. *Information Society.* **20** (5) 313-325.

Bellotti, V. (1997). *Design for privacy in multimedia computing and communications environments in technology and privacy: The new landscape.* Rotenberg, M., and P.E. Agre (Eds). MIT Press, Cambridge, Massachusetts.

Benbasat, I., and A. S. Dexter. 1986. An investigation of the effectiveness of color and graphical information presentation under varying time constraints. *Management Information Systems Quarterly* **10** (1) 59–83.

Benbasat, I., Dexter, A. S. & Todd, P. (1986). An experimental program investigating color-enhanced and graphical information presentation: an integration of the Findings, *Communication of the ACM*, 29 1094 -1105.

Bennett, C.C. (1967). What price privacy? *American Psychologist*, **22** (5) 371-376.

Berendt, B. Gunther, O. & Spiekermann, S. (2005). Privacy in E-Commerce: Stated Preference Vs. Actual Behavior. *Communications of the ACM.* **48** (4) 101-106.

Berghel, H. (2000). Identify Theft, Social Security Numbers, and the Web. *Communications of the ACM.* **43** (2) 17.

Bettman, J. R. & Zins, M.A. (1979). Information Format and Choice Task Effects in Decision Making," Journal of Consumer Research, **6** 141-53.

Bettman, J.R. (1973). Perceived Risk and Its Components: A Model and Empirical Test. *Journal of Marketing Research* **10** (2) 184-19.

Bhattacherjee, A. (2002). Individual trust in online firms: scale development and initial test, *Journal of Management Information Systems.* **19** (1) 211–241

Bignoux, S. (2006). Short-Term Strategic Alliances: A Social Exchange Perspective. *Management Decision.* **44** (5) 615-627.

Blau P.M. (1964) *Exchange and power in social life*. John Wiley and Sons Inc. New York.

Boer, H., & Seydel, E.R. (1996). "Protection motivation theory." In M. Connor and P. Norman (Eds.) *Predicting Health Behavior*. Buckingham: Open University Press

Boritz, J. E. , & No, W.G. (2006). Internet Privacy Research: Framework, Review and Opportunities Available at SSRN: http://ssrn.com/abstract=908647

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

Brown, J. Broderick, A.J., & Lee, N. (2007). Word of mouth communication within online communities: conceptualizing the online Social network. *Journal of Interactive Marketing*. **21** (3) 2-20.

Bumgarner, B. (2007). You have been poked: Exploring the uses and gratification of Facebook among emerging adults. *First Monday*, **12** (11).

Campbell, A. J. (1997). Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy. *Journal of Direct Marketing.* **11** (3) 44-58.

Cao, Y., Theune, M., & Nijholt, A. (2009). Decision making with a time limit: the effects of presentation modality and structure. In *European Conference on Cognitive Ergonomics: Designing beyond the Product --- Understanding Activity and User Experience in Ubiquitous Environments,* Finland.

Card, S. K., Moran, T. P., & Newell, A. (1983). *The Psychology of Human-Computer Interaction.* Lawrence Erlbaum Associates, Hillsdale, NJ.

Carroll, N. V., Chanaporn, S., & Fincham, J. E.. (1986). Perceived Risks and Pharmacists' Generic Substitution Behavior. The Journal of Consumer Affairs. 20 (1) 36-48.

Carter, L.F., (1947). An experiment on the design of tables and graphs used for presenting numierical data. *Journal of Applied Psychology*, **31** 640-650.

Carter, R.C. (1982). Visual search with colour. *Journal of Experimental Psychology: Human Perception and Performances*, **8** 127 - 136.

Carter, R.C., (1982). Visual search with color. *Journal of Experimental Psychology: Human Perception and Performance*, **8** (1) 127-136.

Cases, A.S. (2002). Perceived Risk and Risk Reduction Strategies in Internet Shopping. International Review of Retail. *Distribution and Consumer Research.* **12** (4) 375–394.

Cates, J.A., Dian, D.A., & Schnepf, G.W. (2003). Use of protection motivation theory to assess fear of crime in rural areas. *Psychology, Crime and Law,* **9** (3) 2003

Cazier, J. H., Shao, B. B. M., & St. Louis, R. D. (2002). Personal privacy preferences in e-business: a focus on trust and value compatibility. *Eight Americas conference on Information Systems.* August 9-11 Dallas, Texas.

Chellappa, R.K. (2002). Consumers' Trust in Electronic Commerce Transactions: The Role of Perceived Privacy and Perceived Security. Available at http://www.bus.emory.edu/ram/Papers/sec-priv.pdf, 2002.

Chen, Z., & Dubinsky, A.J. (2003). A conceptual model of perceived customer value in e-commerce: A preliminary investigation. *Psychology & Marketing.* **20** (4) 323-347.

Chenoweth, T. , Minch, T. & Gattiker, T. (2009).Application of Protection Motivation Theory to Adoption of Protective Technologies *Proceedings of the 42nd Hawaii International Conference on System Sciences* January, 5-8, Waikoloa, Hawaii.

Chin, W. W.,&Newsted, P. R. (1999). "Structural equation modeling analysis with small samples using partial least squares", In R. H. Hoyle (Ed.), Statistical strategies for small sample research, Thousand Oaks, CA: Sage

Chin, W.W., Marcolin, B.L., & Newsted, P.R. (1996). A partial least squares latent variable modeling Approach for measuring interaction effects: Results from a monte carlo simulation study And voice mail emotion/adoption study, *Proceedings Of The Seventeenth International Conference On Information Systems,* December 16-18, Cleveland, Ohio.

Chin, W.W., Marcolin, B.L., & Newsted, P.R. (2003). A partial least squares latent variable modeling approach for measuring interactions, *Information Systems Research,* **14** (2).

Cho, J. (2004). Likelihood to abort an online transaction: influences from cognitive valuations, attitudes, and behavioral variables. *Information & Management.* **41** 827-838.

Cho, J., & Lee, J. (2006). An integrated model of risk and risk-reducing strategies. *Journal of Business Research*. **59** (1) 112.

Choi, J., & Geistfeld, L.V. (2004). A cross-cultural investigation of consumer e-shopping adoption. *Journal of Economic Psychology.* **25** 821–838.

Cismaru, M., & Lavack, A.M. (2006). Marketing communications and protection motivation theory: Examining consumer decision-making, *International Review on Public and Nonprofit Marketing.* **3** (2) 9-24.

Collins, J.D.W. (2007). Toothless HIPAA: Searching For a Private Right of Action to Remedy Privacy Rule Violations. *Vanderbilt Law Review.* **60** (1) 199-234.

Connelly, K. (2007) Do I Do What I Say?: Observed Versus Stated Privacy Preferences, *International Conference on Human-Computer Interaction* September 10-14, Rio de Janeiro, Brazil.

Cox, D.F. (1967). Risk handling in consumer behavior. In Cox, D.F (Ed.). *Risk taking and information handling in consumer behavior* Boston, Graduate School of Business Administration Harvard University. 23-33.

Cranor, L.F., Reagle, J. & Ackerman, M.S. (1999). Beyond Concern: Understanding Net user's Attitudes About Online Privacy. *AT&T Labs-Research Technical Report TR 99.4.3.* Retrieved March 9, 2004 from http://www.research.att.com/library/trs/99/99.4/

Culnan, M. J. (1993). "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use. *MIS Quarterly*. **17** (3) 341-364.

Culnan, M. J. (1995). Consumer awareness of name removal procedures: implications for direct marketing. *Journal of Direct Marketing*. **9** 10-19.

Culnan, M. J. (1999). Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission. Retrieved April 1, 2004 from http://www.msb.edu/faculty/culnanm/gippshome.html.

Culnan, M. J. (2000). Protecting Privacy online: Is Self-regulation working. *Journal of Public Policy & Marketing*. **19** (1) 20-27.

Culnan, M. J., & Armstrong, P.K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*. **10** (1) 104-115.

Culnan, M. J., & Bies, R. J. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues*. **59** (2) 323-342.

Cunningham, S.M. (1967). "The major dimensions of perceived risk" In Cox, D.F. (Ed)., *Risk taking and information handling in consumer behavior,* Boston Graduate school of business administration Harvard University 23-33.

Danna, A., & Gandy, O.H. (2002) All That Glitters is Not Gold: Digging Beneath the Surface of Data Mining, *Journal of Business Ethics.* **40** (4) 373-386.

Das, T.L., Teng, B.S. (2004). The risk-based view of trust: a conceptual framework. *Journal of Business and Psychology*, **19** (1) 85-116.

Davis, C.N. (2005). Reconciling Privacy and Access Interests in E-Government. *International Journal of Public Administration,* **28** (7) 567.

Davison, R. M., Clarke, R., Smith, J. Langford, D., & Kuo, K. Y. (2003). Information privacy in a globally networked society: implications for IS research. *Communications of the Association for Information Systems,* **12** 341-365.

De George, R. T. (1999). Business Ethics and the Information Age. *Business and Society Review*, **104** (3) 261-278.

Debatin, B., Lovejoy, J.P., Horn, A.K. & Hughes, B.N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communications*, **15**(1) 83-108.

Decew, J. (2006). Privacy. In *Standford Encyclopedia of Philosophy*. Ed. Zalta, E.N. Accessed August 14, 2007. from http://plato.stanford.edu/entries/privacy/

Dickson, G.W.. DeSanctis, G., & McBride, D.J. (1986). Understanding the effectivess of computer graphics for decision support: A cumulative experimental approach. *Communications of the ACM, **29*** (1) 40-47.

Dinev, T. & Hart P. (2006). Extended privacy calculus model for e-commerce transactions. *Information Systems Research.* **17** (1) 61-80

Dinev, T. & Hart, P. (2002). Internet Privacy Concerns and Trade-off Factors – Empirical Study and Business Implications, *International Conference On Advances In Infrastructure For E-Business*, L'Aquila, Italy.

Dinev, T. and Hu, Q. 2007. The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems*. **8** (7) 386-408.

Dinev, T. and P. Hart, P. (2003). Privacy Concerns and Internet Use: A Model of Trade-off Factors, *Academy of Management Meeting*, Seattle. Retrieved November 20, 2005 from http://wise.fau.edu/~tdinev/publications/aom2003.pdf.

Dinev, T., Bellotto, M., Hart, P., Colautti, C., Russo, V., & Serra, I. (2005). Internet Users' Privacy Concerns and Attitudes towards Government Surveillance – An Exploratory Study of Cross-Cultural Differences between Italy and the United States. *18th Bled e-commerce conference*, June 6-8, Bled, Slovenia.

Doolin, B., Dillon, S., Thompson, F., & Corner, J.L. (2005). Perceived Risk, the Internet Shopping Experience and Online Purchasing Behavior. *Journal of Global Information Management*, **3** (2) 66-89

Douglas, M. (1992). *Risk and Blame: Essays In Cultural Theory*, Routledge: London.

Dowling, G., & Staelin, R. (1994). A Model of Perceived Risk and Intended Risk-Handling Activity. *Journal of Consumer Research.* **21** (1) 119-125.

Dunfee, T. W., Smith, N. C., & Ross, W. T. Jr. (1999). Social contracts and marketing ethics. *Journal of Marketing*. **63** (3) 14-32.

Dwyer, C., Hiltz, S., & Passerini, K. (2007). Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace. *Proceedings of the Americas Conference of Information Systesm.* August 9-12, Keystone Colorado.

Eagly, A. H. and S. Chaiken. (1993). *The psychology of attitudes*. Fort Worth, TX: Harcourt, Brace, Jovanovich.

Earp, J. B. & Anton, A. I. (2004). Addressing end-user concerns. *Proceedings of the Tenth Americas Conference on Information Systems.* August 6-8, New York, New York.

Eddy, E. R., Stone, D. L. & Stone-Romero, E. F. (1999). The effects of information management policies on reactions to human resource information systems: an integration of privacy and procedural justice perspectives. *Personnel Psychology.* **52** (2) 335-358.

Ellison, N. B., Steinfeld, C., & Lampe, C. (2007). The benefits of Facebook ‘‘Friends:’’ Social capital and college students’ use of online social network sites. *Journal of Computer-Mediated Communication,* **12** (4)

EPIC (2003). Excerpt from Introduction to EPIC's "Privacy and Human Rights 2003: Threats to Privacy" available at http://www.privacyinternational.org/survey/phr2003/threats.htm

EPIC (2007). Social networking privacy. Accessed September 10, 2007 from www.epic.org/privacy/socialnet

Featherman, M.S. & Pavlou, P.A. (2003) Predicting e-Services Adoption: A Perceived Risk Facets Perspective. *International Journal of Human-Computer Studies.* **59** (4) 451-474.

Federal Trade Commission. (2000) *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress. Retrieved November 15, 2005 from http://www3.ftc.gov/reports.*

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

Folkman, S., & Lazarus, R. S. (1980). An analysis of coping in a middleaged community sample. *Journal of Health and Social Behavior*. **21** 219-239.

Forlani, D., & Mullins, J.W. (2000). Perceived risks and choices in entrepreneurs' new venture decisions. *Journal of Business Venturing*. **15** (4) 305

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

Fox, R. (2000). The cursor who spied me. *Communications of the ACM*. *43* (2) 9.

Fraenkel, O.K. (1968). Privacy and Freedom (Review). *Annals of the American Academy of Political and Social Science.* ***377*** 196-197.

Friedman, B., Kahn, P.H. Jr., Daniel C. Howe. (2000). Trust Online. *Communications of the ACM*. **43** (2) 34.

Fruin, D. J.; Pratt, C., & Owen, N. (1992). Protection Motivation Theory and Adolescents' Perceptions of Exercise. *Journal of Applied Social Psychology***. 22** (1) 55-69.

Ganesan, S. (1994). Determinants of long-term orientation in buyer–seller relationships, *Journal of Marketing*. **58** 1–19.

Garbarino, E., & Strahilevitz, M. (2004). Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation. *Journal of Business Research.* **57** 768– 775.

Gefen D. and Straub, D.W., (2004). Consumer Trust in B2C e-Commerce and the Importance of Social Presence: Experiments in e-Products and e-Services, O*mega: The International Journal of Management Science*. **32** (6) 407-424.

Gefen, D. (2000). E-Commerce: The Role of Familiarity and Trust, *Omega.* **28** 725-737.

Gefen, D., & Straub , D. (2005). A practical guide to factorial validity using Pls-graph: tutorial and annotated example, *Communication of the Association for Information Systems,* **16** 91-109

Gefen, D., Straub, D.W., & Boudreau, M.C. (2000) Structural Equation Modeling Techniques and regression: Guidelines for research practice. *Communications of AIS,* **7** (7) 1-78.

Gibson, S. (2005). Spyware was Inevitable. *Communications of the ACM*. **48** (8) 37-39.

Gindin, S. E. (1997). Lost and found in cyberspace: Informational privacy in the age of the Internet. *San Diego Law Review.* **34** 1153-1223.

Glenn, C. L. (2000). Protecting Health Information Privacy: The case for self-regulation of electronically held medical records. *Vanderbilt Law Review*. **53** (5), 1605- 1636.

Goodhue, D., Lewis, W., & Thompson, R. (2007). Statistical Power in Analyzing Interaction Effects: Questioning the Advantage of PLS with Product Indicators, *Information Systems Research,* **18** (2) 211-227.

Govani, T. & Pashley, H. (2005). Student Awareness of The Privacy Implications When Using Facebook. Accessed July 11 2007 From Http://Lorrie.Cranor.Org/Courses/Fa05/Tubzhlp.Pdf.

Graham, J. P. (1987). Privacy, computers, and the commercial dissemination of personal information. *Texas Law Review.* **65** (7) 1395-1440.

Greening, L. (1997). Adolescents' cognitive appraisals of cigarette smoking; an application of the protection motivation theory, *Journal of Applied Social Psychology,* **27** 1972-1987.

Greening, L. (1997). Risk perception following exposure to a job-related electrocution accident: The mediating role of perceived control. *Acta Psychologica.* **95** (3) 267-277.

Gross, R., & Acquisti, A. (2005). Information Revelation and Privacy In Online Social Networks. In *Proceedings of WPES'05*, Alexandria, VA, 71-80.

Grover, V., Hall,. Rosenberg, S. (1998). The Web of Privacy: Business in the Information Age. *Business Horizons.* **41** (4) 5-11.

Grupe, F. H. (1995). Commercializing public information: a critical issue fro governmental IS professionals. *Information and Management.* **28** 229-241.

Hale, R. (2001). Federal Privacy Regulation of Internet Credit Card Advertising and Solicitation. *Journal of Internet Law.* **4** (8) 1-12.

Hall, H. (2003). Borrowed theory applying exchange theories in information science research. *Library & Information Science Research.* **25** 287-306

Hann, I. H., Hui, K. L., Lee, T. S. & Png, I.P.L. (2002a). Online information privacy: measuring the cost-benefit trade-off. *Twenty-Third International Conference on Information Systems.* December 10-13, Queensland , Australia.

Hann, I. H., Hui, K. L., Lee, T. S. & Png, I.P.L. (2002b). The value of online information privacy: evidence from the USA and Singapore. Retrieved June 22, 2004 from http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf.

Hann, I.H., Hui, K.L., Lee, T.S, & Png, I.P.L. (2003). The Value of Online Information Privacy: An Empirical Investigation. *Economics Working Paper Archive At WUSTL # 0304001.*

Hart, P., & Dinev, T. (2002). Measuring Antecedents and Trade-Offs to Internet Privacy, *Academy of Management Meeting*, Colorado. Retrieved November 20, 2005 from http://wise.fau.edu/~tdinev/publications/tradeoffs.pdf

Hatala, J.P. (2006). Social Network Analysis in Human Resource Development: A New Methodology. *Human Resource Development Review.* **5** (1) 45-72.

Herath, T., & Rao, H.R. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations, *European Journal of Information Systems* **18** (2) 106-125.

Hiller, J. S. and Belanger, F. (2001). "Privacy Strategies for Electronic Government," in Abramson, M.A. and Means, G.E. (Eds). *E-Government 2001***,** Rowman & Littlefield Publishers: New York, New York.

Hine, C., Eve, J. (1998). Privacy in the Marketplace. *The Information Society.* **14** 253-262.

Hochbaum, G., Kegels, S. & Rosenstock, I. (1952). Health Belief Model, developed while working in the U.S. Public Health Services.

Hoffman, D. L. (2003). The Consumer Experience: A Research Agenda going Forward. FTC Public Workshop1: Technologies for Protecting Personal Information: The consumer Experience. Panel: Understanding How Consumers Interface with Technologies Designed to Protect Consumer Information. May 14, 2003.

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999a). Information Privacy in the Marketplace: Implications for the Commercial Uses of Anonymity on the Web. *The Information Society*. **15** (2) 129-140.

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999b). Building Consumer Trust Online. *Communications of the ACM*. **42** (4) 80-85.

Homans, G.C. (1958). Social Behavior as Exchange. *The American Journal of Sociology*. **63** (6) 1858-1958.

Homburg, A., & Stolberg, A. (2006). Explaining pro-environmental behavior with a cognitive theory of stress. *Journal of Environmental Psychology*. **26** (1) 1-14.

Hong, W., Thong, J. Y. L., & Tam, K. Y. (2005).The Effects of Information Format and Shopping Task on Consumers' Online Shopping Behavior: A Cognitive Fit Perspective, Journal of Management Information Systems **21** (3) 149-184.

Hui, K.L., Tan, B.C.Y., & G, C.Y. (2006). Online information disclosure: motivators and measurements. *ACM Transactions on Internet Technology*. **6** (4) 415-441.

Jackson, L. A., Von-Eye, A., Barbatsis, G., Biocca, F., Zhao, Y., & Fitzgerald, H. E. (2003). Internet attitudes and Internet use: some surprising findings from the HomeNetToo project. *International Journal of Human-Computer Studies*. **59** 355-382.

Jacoby, J. and Kaplan, L.B. (1972), "The components of perceived risk)", in Venkatesan, M. (Ed.), *Proceedings of the 3rd Annual Conference of the Association for Consumer Research* 382-93.

Janis, I. L., & Feshbach, S. (1953). Effects of fear-arousing communications. *Journal of Abnormal and Social Psychology*, **48** 78-92.

Jarvenpaa, S., & Dickson, G. (1988). Graphics and managerial decision making, research based guidelines. *Communications of the ACM*, **21** (6) 764-7774

Jarvenpaa, S. L. (1989). The effect of task demands and graphical format on information processing strategies .*Management Science* **35** (3) 285–303.

Jarvenpaa, S.L., & Tractinsky, N. (1999). Consumer trust in an internet store: a cross-cultural validation, *Journal of Computer Mediated Communication.* **5** (2).

Jarvenpaa, S.L., Tractinsky, N, &Vitale, M. (2000). Consumer Trust In An Internet Store. *Information Technology and Management.* **1** (1-2) 45.

Johnson, C., (1974). Privacy as personal control. In *Man-Environment Interactions: Evaluations and applications*, Washigton, D.C.: Environmental Design Research.

Johnson, E. J., and Payne, J. W. (1985). Effort and Accuracy In Choice, *Management Science*, **31 (**4) 395-414.

Johnston, A. C. (2006). An Empirical Investigation of the Influence of Fear Appeals on Attitudes and Behavioral Intentions Associated with Recommended Individual Computer Security Actions. Doctoral Thesis. UMI Order Number: AAI3213966., Mississippi State University.

Johnston, A., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study, *MIS Quarterly*, **34** (3) 549-566.

Joinson, A. N. (2008). Looking at, looking up or keeping up with people?: motives and use of facebook. In *Proceeding of the Twenty-Sixth Annual SIGCHI Conference on Human Factors in Computing Systems.* April 5-10, Florence, Italy.

Jones, H., & Soltren, J.H. (2005). Facebook: Threats to privacy. Available at http://www.swiss.ai.mit.edu/6095/student-papers/fall05-papers/facebook.pdf

Joshi, J.B.D., Ghafoor, A., Aref, W.G., & Spafford, E.H. (2002). "Digital Government Security and Privacy Challenges" In McIver, W.J.Jr., & Elmagarmid, a.K. (Eds). Advan*ces in Digital Government: Technology, Human Factors, and Policy*. Kluwer, Boston 121-136.

Kamis, A., M. Koufaris, & Stern, T. (2008). Using an attribute-based DSS for user-customized products online: An experimental investigation, *MIS Quarterly*, **32** (1) 159-177.

Kehoe, C., Pitkow, J., Sutton, K., Agarwal, G., & Rogers, J. D. (1999). Results of GVU's Tenth World Wide Web User Survey. Retrieved March 31, 2005 from http://www.gvu.gatech.edu/user_surveys/survey-1998-10/tenthreport.html.

Kelly, E. P., & Unsal, F. (2002). Health information privacy and e-healthcare. *International Journal of Healthcare Technology and Management.* **4** (1/2) 41- 52.

Kelton, A.S., Pennington, R.R., & Tuttle, B.M., (2003). The Effects of Information Presentation Format on Judgment and Decision Making: A Review of the Information Systems Research, *Journal of Information Systems,* **24** (2) 79-105.

Kelvin, P. (1973). A social psychological examination of privacy. *British Journal of Social Clinical Psychology* **12** 284–251.

Kennedy, M., Te'eni, D., & Treleaven, J.B. (1998). Impacts of decision task, data and display on strategies for extracting information, *International Journal of Human-computer Studies,* **48** 159-180.

Kim, J., Hahn, J., & Hahn, H. (2000). How do we understand a system with (so) many diagrams? Cognitive integration processes in diagrammatic reasoning, *Information Systems Research.* **11** (3) 284

Kimery, K.M., & McCord, M. (2002). Third party assurances: Mapping the road to trust in e-retailing. *Journal of Information Technology Theory and Application.* **4** (2) 63-83.

Kirsh, E. M., Phillips, D. W., & McIntyre, D. E. (1996). Recommendations for the evolution of cyber law. *Journal of Computer-Mediated Communication* **2** (2).

Kling, R., Lee, Y. C., Teich, A., & Frankel, M. S. (1999). Assessing Anonymous communication on the Internet: Policy Deliberations. *The Information Society.* **15** 79-90.

Koller, M. (1988). Risk As A Determinant of Trust. *Basic and Applied Social Psychology.* **4** 265-276.

Kollock, P. (1994). The Emergence of Exchange Structures: An Experimental Study of Uncertainty, Commitment, and Trust. *The American Journal of Sociology.* **100** (2) 313-345.

Kuhlmeier, D. & Knight, G. (2005). Antecedents To Internet-Based Purchasing: A Multinational Study. *International Marketing Review.* **22** (4) 460.

LaRose, R., & Rifon, N.J. (2007). Promoting i-Safety: Privacy Warning Boxes, Privacy Seals and Online Privacy Behavior, *The Journal of Consumer Affairs.* **41** (1) 127-149.

Lee, Y. and Larsen, K. (2009). Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-malware Software. *European Journal of Information Systems.* **18** 177-187.

Lenhart, A., & Madden, M. (2007). Teens, privacy, & online social networks. *Pew Internet and American Life Project Report.* Accessed July 30, 2007 from http://www.pewinternet.org/pdfs/PIP_Teens_Privacy_SNS_Report_Final.pdf

Lewis, D. P. (1988). Protecting your confidential information. *Computer law and security report.* **4** (4) 28-32.

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

Liebermann, Y., & Stashevsky, S. (2002). Perceived risks as barriers to Internet and e-commerce usage, *Qualitative Market Research.* **5** (4) 291.

Lohse, G.L. (1997). The role of working memory on graphical information processing. *Behaviour & Information Technology*, **16** (6) 297-308.

Lopez, X. R. (1994). Balancing information privacy with efficiency and open access: a concern of government and industry. *Government Information Quarterly*. **11** (3) 255-260.

Lu, Y., Tan, B., & Hui, K.L. (2004). "Inducing Customers to Disclose Personal Information to Internet Businesses with Social Adjustment Benefits" *Proceedings of the International Conference of Information Systems.*

Luhmann, N. (1979) Trust and power. John Wiley and Sons Inc. Chichester.

Luo, X. (2002). Trust production and privacy concerns on the Internet a framework based on relationship marketing and social exchange theory. *Industrial Marketing Management.* **31** 111-118.

Ma, G.X., Fang, C.Y., Shive, S.E., & Toubbeh, J. (2007). Risk Perceptions and Barriers to Hepatitis B Screening and Vaccination among Vietnamese Immigrants. *Journal of Immigrant and Minority Health*. **9** (3) 213-221.

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

Mason, R. O. (1986). Four Ethical Issues of the Information Age. *MIS Quarterly*. **10** (1) 1-10.

Masuda, Y.(1979). Privacy in the future information society. *Computer Networks*. **3** (3) 164-170

Mayer, R. J., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *Academy of Management Review.* **20** 709-734.

McGinity, M. (2000). Surfing your turf. *Communications of the ACM*. **43** (4) 19-21.

McMath, B. F., & Prentice-Dunn, S. (2005). Protection motivation theory and skin cancer risk: The role of individual differences in responses to persuasive appeals. *Journal of Applied Social Psychology.* **35** 621-643.

Meeks, B. N. (1999). The Privacy Hoax. *Communications of the ACM*. **42** (2) 17-20.

Meeks, B. N. (1997). Privacy lost, anytime, anywhere. *Communications of the ACM*. **40** (8), 11-14.

Meservy, M. & Banks, S.M. (2010). Risky Behavior in Online Social Media: Protection Motivation and Social Influence, *Proceedings of the Americas Conference on Information Systems* August 12-15, Lima, Peru.

Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. *Communications of the ACM*. **38** (12) 65-74.

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: corporate management and national regulation. *Organization Science.* **11** (1) 35-58.

Miller, G.A. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological Review*, **63** 81-97

Milne, G R., Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy & Marketing.* **12** (2) 206-215.

Milne, G. R. (2000). Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue. *Journal of Public Policy & Marketing.* **19** (1) 1-7.

Milne, G., & Culnan, M.J. (2004). Strategies for Reducing Online Privacy Risks: Why Consumers Read [Or don't Read] Online Privacy Notices. *Journal of Interactive Marketing.* **18** (3) 15-29.

Milne, G.R., & Rohm, A.J. (2000). Consumer Privacy and Name removal across direct marketing channels: exploring opt-in and opt-out alternatives. *Journal of Public Policy and Marketing,* **19** (2) 238-24.

Milne, G.R., Rohn, A.J., Bahl, S. (2004). Consumers' Protection of Online Privacy and Identity. *The Journal of Consumer Affairs.* **38** (2) 217-223.

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

Mitchell, V.W. (1999). Consumer Perceived Risk: Conceptualisations and Models. *European Journal of Marketing.* **33** (1-2) 163 – 195.

Miyazaki, A. D., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *The Journal of Consumer Affairs.* **35** (1) 27-55.

Molm, L. D., Takahashi, N., & Peterson, G. (2000). Risk and Trust in Social Exchange: An Experimental Test of a Classical Proposition. *The American Journal of Sociology.* **105** (5) 1396-1427.

Molm, L.D. (2001). "Theories of social exchange and exchange networks." In G. Ritzer and B. Smart. (Eds), *Handbook of Social Theory.* Sage Publications. London.

Morgan, RM., & Hunt, S.D. (1994). The commitment-trust theory of relationship marketing, *Journal of Marketing Research.* **29** 20-38.

Nabeth, T. (2005). Understanding the Identity Concept in the Context of Digital Social Environments. *INSEAD CALT (the Centre for Advanced Learning Technologies)*

Nisenoff, N., Bishop, E., & Clayton, A. (1979). The privacy of computerized records- the Swedish experience and possible US policy impacts. *Information Processing and Management*. **15** (4) 205-211.

Norberg, P.A.. Horne, D.R., & Horne, D.A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors. *The Journal of Consumer Affairs.* **41** (1).

Nowak, G. J., & Phelps, J. (1992). Understanding Privacy Concerns: An Assessment of Consumers' Information-Related Knowledge and Beliefs. *Journal of Direct Marketing.* **6** (4) 28-39.

Nunnally, J. C. (1978). *Psychometric Theory*. New York, NY: McGraw-Hill

O'Brein, D. G., Yasnoff, W. A. (1999). Privacy, confidentiality, and security in information systems of state health agencies. *American Journal of Preventive Medicine*. **16** (4) 351-358.

Odlyzko, A.. (2003). Privacy, economics, and price discrimination on the Internet. *Fifth International Conference on Electronic Commerce.* Nice, France.

Oliver, H. (2002). Email and Internet monitoring in the Workplace: information privacy and contracting-out. *The Industrial Law Journal.* **31** (4) 321-352.

Olivero, N., Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology*. **25** 243-262.

Otjacques, B. Hitzelberger, P., & Feltz, F. (2007) Interoperability of E-Government Information Systems: Issues of Identification and Data Sharing. *Journal of Management Information Systems.* **23** (4).

Paterson, R. J., & Neufeld, R.W. J. (1995). What Are My Options? : Influences of Choice Availability on Stress and the Perception of Control, *Journal of Research in Personality*, **29** (2) 145-167.

Pavlou, P. A., Liang, H. &Xue, Y. (2005), Understanding and Mitigating Uncertainty in Online Environments: A Longitudinal Analysis of Trust and Social Presence, P*roceedings of the Academy of Management Conference*, Honolulu, HI

Pavlou, P. A., Liang, H. &Xue, Y. (2007), Understanding and Mitigating Uncertainty in Online Environments: A Principal-Agent Perspective, *MIS Quarterly.* **31** (1) 105-136.

Pavlou, P.A. (2003). Consumer Acceptance of Electronic Commerce - Integrating Trust and Risk, With The Technology Acceptance Model. *International Journal of Electronic Commerce.* **7** (3) 69-103.

Pechmann, C., Zhao, G.Z., Goldberg, M.E., & Reibling, E.T. (2003). What to convey in antismoking advertisements for adolescents: The use of protection motivation theory to identify effective message themes. *Journal of Marketing.* **67** (2) 1-18.

Pempek, T.A., Yermolayeva, Y.A., & Calvert, S.L. (2009). College students' social networking experiences on Facebook, *Journal of Applied Developmental Psychology*, **30** 227-238.

Peslak, A.R. (2006). Papa revisited: a current empirical study of the mason framework. *The Journal of Computer Information Systems*. **46** (3) 117-124.

Peter, J.P. & Tarpey, L.X. (1975). A comparative analysis of three consumer decision strategiess'. *Journal of Consumer Research.* **2** 29-37.

Peterson, S. B. (1995). Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete? *Federal Communications Law Journal*.

Petrison, L. A., & Wang, P. (1995). Exploring the dimensions of consumer privacy: an analysis of converge in British and American media. *Journal of Direct Marketing.* **9** (4) 19-37.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness To Provide Personal Information. *Journal of Public Policy & Marketing.* **19** (1) 27-42

Prentice-Dunn, S. and R. Rogers. (1986). Protection motivation theory and preventive health: Beyond the health belief model. *Health Education Research* **1** 153-161

Prentice-Dunn, S., Mcmath, B.F., & Cramer, R.J. (2009). Protection Motivation Theory and Stages of Change in Sun Protective Behavior, *Journal of Health Psychology*, **14** (2) 297-305.

Raab, C. D., Bennett, C. J. (1998). The Distribution of Privacy Risks: Who Needs Protection. *The Information Society.* **14** 263-274.

Ray, I., Zhang, H. (2008). Experiences In Developing A Fair-Exchange E-Commerce Protocol Using Common Off-The-Shelf Components. *Electronic Commerce Research and Application.* **6** (2).

Reichheld, F.F., & Schefter, P. (2000) E-Loyalty: Your Secret Weapon On The Web. *Harvard Business Review.* 105-115

Resnick, M. L. and Montania, R. (2003). Perceptions of Customer Service, Information Privacy, and Product Quality From Semiotic Design Features in an Online Web Store. *International Journal of Human-Computer Interaction.* **16** (2) 211-235.

Rindfleisch, A., & Crockett., D.X.,(1999) Cigarette smoking and perceived risk: A multidimensional investigation. *Journal of Public Policy & Marketing.* **18** (2) 159-172.

Rindfleisch, T. C. (1997). Privacy, information technology, and health care. *Communications of the ACM.* **40** (8) 92-100.

Ring, PS., and Van de Ven, A.H.(1994). Developing processes of cooperative inter-organizational relationships. *Academy of Management Review.* **19** 90-118.

Rippetoe, P.A., & Rogers, R.W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology.* **52** (3) 596-604.

Rogers, R. W. (1983). "Cognitive and physiological processes in attitude change: A revised theory of protection motivation." In Cacioppo, J., & Petty R. (Eds). *Social Psychophysiology Guilford Press.* New York 153-176.

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

Rohm, A.J., & Milne, G.R. (2004). Just what the doctor ordered: The role of information sensitivity and trust in reducing medical information privacy concern. *Journal of Business Research.* **57** (9) 1000-1011.

Roselius, T. (1971). Consumer ranking of risk reduction methods. *Journal of Marketing,* **35 (**1) 56-61.

Roskos-Ewoldsen, D., Yu, H. J., & Rhodes, N. (2004). Fear appeal messages effect accessibility of attitudes toward the threat and adaptive behaviors. *Communication Monographs*, **71** 49-69.

Rotenberg, M. (1994). Privacy protection. *Government information Quarterly*. **11** (3) 253-254.

Rousseau, D.M., Sitkin, S.M., Burt, R.S., & Camerer C. (1998). Not So Different After All: A Cross-discipline View of Trust. *Academy of Management Review.* **23** (3) 393-404.

Schlosser, A.E., White, T.B. & Lloyd, S.M. (2006). Converting web site visitors into buyers: how web site investment increases consumer trusting beliefs and online purchase intentions. Journal of Marketing, 70 133-148.

Schwaig, K.S., Kane, G.C., & Storey, V.C. (2006). Compliance to the fair information practices: How are the Fortune 500 handling online privacy disclosures? *Information & Management.* **43** 805-820.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of Privacy Concern Among Online Consumers. *Journal of Public Policy & Marketing*. **19** (1) 62-74.

Sipior, Janice C., Burke T. Ward. (1995). The ethical and legal quandary of Email privacy. *Communications of the ACM.* **38** (12) 48-55.

Siponen, M., Pahnila, S., & Mahmood, A. (2006). 'Factors Influencing Protection Motivation and IS Security Policy Compliance," *Proceedings of the International Conference on Innovations in Information Technology.* 1-5.

Slovic, P. (1999). Trust, Emotion, Sex, Politics, and Science: Surveying The Risk-Assessment Battlefield. *Risk Analysis.* **19** (4) 689-701.

Smith, H J. (2001). Information privacy and marketing: What the US should (and shouldn't) learn from Europe. *California Management Review.* **43** (2) 8-34.

Smith, H. J., Milberg, S. J., Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly*. **20** (2) 167-196.

Speier, C. (2006). The influence of information presentation formats on complex task decision-making performance. *International Journal of Human-computer Studies*, **64** 115-1131.

Stainback, R.D. & Rogers, R.W. (1983). Identifying effective components of alcohol abuse prevention programs: effects of fear appeals, message style and source expertise, *International Journal of Addictions.* **18** 393-405.

Stewart, K. A., Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research.* **13** (1) 36-49.

Stone, E.F., Gueutal, H.G., Gardner, D.G., & McClure, S.M. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology.* **68** (3) 459-4687.

Stone, E.R., Yates, J.F., &Parker, A.M. (1997). Effects of Numerical and Graphical displays on Professed risk-taking behavior. *Journal of Experimental Psychology*, **3** (4) 243-256.

Strater, K. & Richter, H. (2007). Examining Privacy and disclosure in a Social Networking Community *Symposium On Usable Privacy and Security (SOUPS)* July 18-20, Pittsburgh, Pennsylvania.

Strauss, J., Rogerson, K. S. (2002). Policies for online privacy in the United States and the European Union. *Telematics and Informatics.* **19** 173-192.

Sturges, J.W. & Rogers, R.W. (1996). Preventive health psychology from a development perspective: An extension of protection motivation theory. *Health Psychology* **15** (3) 158-166.

Stutzman, F. (2006). An evaluation of identity-sharing behavior in social network communities. *Proceedings of the presented at the iDMAa and IMS Code Conference*, Oxford, Ohio.

Tan, S. J. (1999). Strategies for reducing consumers' risk aversion in Internet shopping. *Journal Of Consumer Marketing.* **16** (2) 163-180

Tanner, J.F., J.B. Hunt, and D.R. Eppright. (1991). The protection motivation model: A normative model of fear appeals, Journal of Marketing, **55** 36-45.

Tavani, H. T. (1999). Information privacy, data mining, and the Internet. *Ethics and information Technology*. **1** (2) 137-145.

Taylor, J.W. (1974). The Role of Risk In Consumer Behavior. *Journal of Marketing.* **38** (2) 54-60

Tenenhaus, M., Vinzi, V. E. Chatelin, Y-M., & Lauro, C. (2005). PLS Path Modeling, *Computational Statistics and Data Analysis* **48** (1) 159-205.

Thompson, S.C., Sobolew-Shubin, A., Galbriath, M.C., Schwankovsky, L., & Cruzen, D. (1993) Maintaining Perceptions of Control: Finding Perceived Control In Low-Control Circumstances. *Journal of Personality and Social Psychology.* **64** 293-304.

Todd, P., and Benbasat, I. (1999). Evaluation the Impact of DSS, Cognitive Effort, and Incentives on Strategy Selection, *Information Systems Research* **10 (**4) 356-375.

Treisman, A. (1982), Perceptual grouping and attention in visual search for features and for objects, *Journal of Experimental Psychology: Human Perception and Performance*, **8** 194-214

Tu, C. H. (2002). The relationship between social presence and online privacy. *Internet and Higher Education*. **5** 293-318

Tuerkheimer, F. M. (1993). The under-pinnings of privacy protection. *Communications of the ACM.* **36** (8) 69-74.

Ueltschy, L.C., Krampf, R.F., & Yannopoulos, P. (2004). A Cross-National Study Of Perceived Consumer Risk Towards Online (Internet) Purchasing. *The Multinational Business Review.***12** (2) 59-83.

Umanath, N. S., &Vessey, I. (1994). Multi-attribute data presentation and human judgment: A cognitive fit perspective. *Decision Sciences* **25 (**5/6) 795–824.

Umeh, K. (2004) cognitive appraisals, maladaptive coping, and past behavior in protection motivation. *Psychology and Health.* **19** (6) 719-735.

Van Slyke, C., Shim, J.T., Johnson, R. & Jiang, J., (2006). Concern For Information Privacy, Risk Perception and Online Consumer Purchasing. *Journal of The Association For Information Systems* **7** (6) 415-444.

Vessey, I. (1991). Cognitive Fit: A Theory-Based Analysis of the Graphs Versus Tables Literature. *Decision Sciences* **22** (2) 219-240.

Vessey, I., & Galletta, D. (1991). Cognitive Fit: An Empirical Study of Information Acquisition. *Information Systems Research*, **2** (1) 63-84.

Wacks, R. (1989) *Personal information, privacy, and the law.* Oxford, Oxford university press.

Wang, H., & Wang, C. (1998). Consumer Privacy Concerns about Internet Marketing. *Communications of the ACM.* **41** (3) 63-70.

Ward, S., Bridges, K. & Chitty, B. (2005). Do Incentives Matter? An Examination of On-line Privacy Concerns and Willingness to Provide Personal and Financial Information, *Journal of Marketing Communications.* **11** (1) 21-40.

Warkentin, M., Luo, s., & Templeton, G.F. (2005). A Framework for Spyware Assessment. *Communications of the ACM*. **48** (8) 79-84.

Warren, S. & Brandeis, L., (1890). The Right to Privacy. *Harvard Law Review.* **4** (5) 193-220.

Weible, R.J. (1993). Privacy and data: an empirical study of the influence between web surfers and non-surfers: theoretical and practical implications. In *Proceedings of the conference of the American academy of advertising,* Gainseville FL.

Weinstein, N.D. (2000). Perceived Probability, Perceived Severity, and Health-Protective Behavior, *Health Psychology,* **19** (1) 165-74.

Weisband, S. P., Reining, B. A.. (1995). Managing user perceptions of Email privacy. *Communications of the ACM.* **38** (12) 40-48.

Westin, A. (1967). *Privacy and Freedom. Atheneum*, New York.

White, T.B. (2004). Consumer Disclosure and Disclosure Avoidance: A Motivational Framework. *Journal of Consumer Psychology,* **14** (1,2) 41-51.

Wickens, C. D. and Carswell, C. M. (1995). The proximity compatibility principle: Its psychological function and relevance to display design, *Human Factors*, **37** 473 -494.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs,* **59** 329-349.

Witte, K. (1994). Fear control and danger control: An empirical test of the extended parallel process model. *Communication Monographs,* **61** 113-134.

Witte, K. Cameron, K.A., Mckeon, J.K., & Berkowitz, J.M. (1996). Predicting Risk Behaviors: development and Validation of a Diagnostic Scale, *Journal of Health Communication,* **1** 317–341.

Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior,* **27** 608-632.

Wood, R. E. (1986). Task Complexity: Definition of the Construct. *Organizational Behavior and Human Decision Processes* **37** 60-82.

Woon, M. Y., Low, R.T., & Tan, G.W. (2005). A Protection Motivation Theory Approach to Home Wireless Security, *Proceedings of the International Conference on Information Systems,* Las Vegas, Nevada.

Workman, M. Bommer, W.H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*. **24** 2799-2816**.**

Xiang, Y., Chau, M., Atabakhsh, H., and Chen, H. (2005) Visualizing Criminal Relationships: Comparison of a Hyperbolic Tree and a Hierarchical List, *Decision Support Systems* **41** 69-83.

Xie, E, Teo, H.H, & Wan, W. (2006) Volunteering personal information on the internet: effects of reputation, privacy notices, and rewards on online consumer behavior. *Marketing letter*. **17** 16-74.

Xu, H., Dinev, T., Smith, J.H. & Hart, P. (2008). Examining the formation of individual's privacy concerns: toward an integrative view. *International conference on information Systems.*

Xu, Y., Tan, B. C. Y., Hui, K. L., & Tang, W. K. (2003). Consumer Trust and Online Information Privacy. *Proceedings of the International Conference on Information Systems.* December 14-17, Seattle, Washington.

Yang, S., & Wang, K. (2009)The Influence of Information Sensitivity Compensation on Privacy Concern and Behavioral Intention. *The DATA BASE for Advances in Information Systems.* **40** (1) 38-51.

Yates, J.F., & Stone, E.R. (1992). *Risk taking behavior* John Wiley, Chichester UK.

Yiu, C.S., Grant, K, & Edgar, D. (2007). Factors effecting the adoption of Internet Banking in Hong Kong-implications for the banking sector. *International Journal of Information Management.* **27** (5) 336.

Youn, S. (2005). Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk-Benefit Appraisal Approach. *Journal of Broadcasting & Electronic Media.* **49**

Zigurs, I., & Buckland, B., (1998). A theory of task/technology fit and group support systems effectiveness, *MIS Quarterly*, **22** (3) 313-334.