2012

A Comparison of Users' Personal Information Sharing Awareness, Habits, and Practices in Social Networking Sites and E-Learning Systems

Albert Ball
Nova Southeastern University, al.aball@gmail.com

A Comparison of Users' Personal Information Sharing Awareness, Habits, and Practices in Social Networking Sites and E-Learning Systems

by

Albert L. Ball

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

Graduate School of Computer and Information Sciences
Nova Southeastern University

2012

We hereby certify that this dissertation, submitted by Albert L. Ball, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

_____ _____

Yair Levy, Ph.D. Date
Chairperson of Dissertation Committee

_____ _____

Laurie P. Dringus, Ph.D. Date
Dissertation Committee Member

_____ _____

James Parrish, Ph.D. Date
Dissertation Committee Member

Approved:

_____ _____

Eric S. Ackerman, Ph.D. Date
Interim Dean

Graduate School of Computer and Information Sciences
Nova Southeastern University

2012

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

A Comparison of Users' Personal Information Sharing Awareness, Habits, and Practices in Social Networking Sites and E-Learning Systems

by
Albert L. Ball
October 2012

Although reports of identity theft continue to be widely published, users continue to post an increasing amount of personal information online, especially within social networking sites (SNS) and e-learning systems (ELS). Research has suggested that many users lack awareness of the threats that risky online personal information sharing poses to their personal information. However, even among users who claim to be aware of security threats to their personal information, actual awareness of these security threats is often found to be lacking. Although attempts to raise users' awareness about the risks of sharing their personal information have become more common, it is unclear if users are unaware of the risks, or are simply unwilling or unable to protect themselves.

Research has also shown that users' habits may also have an influence on their practices. However, user behavior is complex, and the relationship between habit and practices is not clear. Habit theory has been validated across many disciplines, including psychology, genetics, and economics, with very limited attention in IS. Thus, the main goal of this study was to assess the influence of users' personal information sharing awareness (PISA) on their personal information sharing habits (PISH) and personal information sharing practices (PISP), as well as to compare the three constructs between SNS and ELS. Although habit has been studied significantly in other disciplines, a limited number of research studies have been conducted regarding IS usage and habit. Therefore, this study also investigated the influence of users' PISH on their PISP within the contexts of SNS and ELS. An empirical survey instrument was developed based on prior literature to collect and analyze data relevant to these three constructs. Path analysis was conducted on the data to determine the influence of users' PISA on their PISH and PISP, as well as the influence of users' PISH on their PISP. This study also utilized ANCOVA to determine if, and to what extent, any differences may exist between users' PISA, PISH, and PISP within SNS and ELS.

The survey was deployed to the student body and faculty members at a small private university in the Southeast United States; a total of 390 responses was received. Prior to final data analysis, pre-analysis data screening was performed to ensure the validity and accuracy of the collected data. Cronbach's Alpha was performed on PISA, PISH, and PISP, with all three constructs demonstrating high reliability. PISH was found to be the most significant factor evaluated in this study, as users' habits were determined to have the strongest influence on their PISP within the contexts of SNS and ELS.

The main contribution of this study was to advance the understanding of users' awareness of information security threats, their personal information sharing habits, and their personal information sharing practices. Information gained from this study may help organizations in the development of better approaches to the securing of users' personal information.

ACKNOWLEDGEMENTS

First and foremost, I want to thank my Lord and Savior, Jesus Christ. He is my salvation and my source of strength and guidance.

This dissertation is dedicated to my wife, Diane. Were it not for your loving guidance, support, and encouragement, accomplishing this dream would not have been possible. I cannot begin to tell you how much you mean to me. I also would like to offer heartfelt thanks to my parents, Donna and Donald Ball, for instilling in me the values and work ethic that were required for successful completion. Finally, a special note of gratitude to the United States Navy Seabees, which instilled in me the “Can Do” attitude.

I would like to thank my dissertation advisor, Dr. Yair Levy, for his leadership, guidance and support throughout this dissertation process. I have learned so much from you. I also want to thank my committee members, Dr. James Parrish and Dr. Laurie Dringus, for their help and support. Thank you all for challenging me and guiding me through this process. I am very grateful.

May God bless you all.

Table of Contents

List of Tables

Tables

2

List of Figures

Figures

Chapter 1

Introduction

Background

Identity theft continues to be a modern day crisis that potentially affects every person who uses the Internet (Anderson, Durbin, & Salinger, 2008; Lai, Li, & Hsieh, 2012). Contributing to this problem is users' risky online sharing of personal information, which has been found to increase the risk of attacks on their personal information (Anderson et al., 2008; Furnell, Tsaganidi, & Phippen, 2008). However, many people find securing their personal information and systems to be cumbersome and frustrating, and obstructs their access to information or online resources (Chipperfield & Furnell, 2010). Although attempts to raise users' awareness about the risks of sharing their personal information have become more common, it is unclear if users are still unaware of the risks, or are simply unwilling or unable to protect themselves. Two main information systems (IS) that are increasingly used to share personal information are social networking sites (SNS) and e-learning systems (ELS). Therefore, it has been suggested that additional research be conducted that investigates users' practices regarding their personal information while using SNS and ELS (Anderson et al., 2008; Chipperfield & Furnell, 2010; Furnell, 2008). This study compared users' personal information sharing awareness (PISA), personal information sharing habits (PISH), and personal information sharing practices (PISP) within SNS and ELS.

This study was organized in the following manner. First, a statement of the specific problem to be researched was presented. Addressed next was the main dissertation goal, research questions, and hypotheses, as well as the relevance and significance of this research. A comprehensive literature review of related areas of research was presented within each of the relevant areas: PISA, PISH, PISP, SNS, and ELS. Next, the specific instruments that were used to measure users' PISA, PISH, and PISP were presented. Specific limitations, delimitations, and barriers were discussed. Finally, the specific data analyses that were used to compare users' PISA, PISH, and PISP were presented, as well as a definition of terms.

Problem Statement

The research problem this study addressed is that, although public awareness of the threat of identity theft has increased substantially, new avenues for identity fraud have contributed to an increasing number of security incidents, including identity theft (Anderson et al., 2008; Furnell, Bryant, & Phippen, 2007; Wu, Andoh-Baidoo, Crossler, & Tanquma, 2011). Although users are generally aware of information security threats to their personal information, they often engage in risky online PISP that may increase the risk of attacks on their personal information (Anderson et al., 2008; Furnell et al., 2008). Identity theft is "the unlawful use of another's personal identifying information" (Bellah, 2001, p. 222). According to Furnell et al. (2007), information security threats are increasing, putting users' personal information at risk. These threats are compounded by the unwillingness or inability of many users to protect themselves from security attacks (Furnell et al., 2008).

These increased threats can be attributed, in part, to risky user online practices related to the sharing of personal information (Furnell, 2008; WSJ, 2010). Moreover, many IS users are willing to accept increased risk in return for convenience (Furnell et al., 2008; WSJ, 2010). For example, due to the varied security requirements associated with different IS, many users store usernames and passwords in their systems for convenience (Furnell et al., 2008). However, they suggested that many users simply lack awareness of the threats that these practices pose to their personal information. Even users who claim to be aware of increased threats to their personal information may not exhibit good information sharing practices (Furnell, 2008). Power and Trope (2006) suggested that users' habits may also have an influence on their practices.

Information security is defined as "the protection of personal data against accidental or intentional disclosure to unauthorized persons, or unauthorized modifications or destruction" (Udo, 2001, p. 165). Information security threats to users' personal information include the breach of information privacy, identity theft, fraud, and other information security threats posed by the unauthorized access and use of personal information (Udo, 2001; Zukowski & Brown, 2007). Furnell (2008) suggested that, although users are aware of information security threats to their personal information, they often have overconfidence in information security protections such as anti-virus and anti-spyware software. Shaw, Chen, Harris, and Huang (2009) defined information security awareness as "the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control" (p. 92). Although users claimed to be aware of security threats to their personal information, Furnell et al. (2007) found that users' actual

awareness of security threats was lacking. They stated that "the awareness of official and mass media efforts to educate the population can be shown to be lacking in engagement and impact" (p. 417).

In recent years, personal information sharing has become common in popular IS such as SNS and ELS (Dwyer, Hiltz, & Passerini, 2007; Ellison, Steinfield, & Lampe, 2011; Furnell, 2008). Boyd and Ellison (2007) defined a social network as

> Web-based services that allow individuals to 1) construct a public or semi-public profile within a bounded system, 2) articulate a list of other users with whom they share a connection, and 3) view and transverse their lists of connections and those made by others within the system. (p. 211)

Users have been found to regularly participate in risky online personal information sharing while using SNS such as Facebook© and MySpace® (Furnell, 2008; Short, 2008). Because of these issues, further investigation into users' security awareness and their PISP has been recommended (Furnell et al., 2007).

Information security threats related to the sharing of personal information also exist within ELS (Cazier, Wilson, & Medlin, 2007; Weippl, 2005). According to Levy and Murphy (2002), an ELS is defined as "the entire technological, organizational, and management system that facilitates and enables students learning via the Internet" (p. 42). Moreover, the types of personal information sharing tools commonly found in SNS, such as discussion boards, wikis, blogs, and other tools are also often used in ELS (Dalsgaard, 2006). According to Short (2008) as well as Li and Poon (2011), many of these tools are often used without knowledge or oversight of the organization's information technology (IT) department or management. As a result, proper security training and precautions

designed to reduce security risks are often not in place (Short, 2008). Most ELS also use basic username and passwords for authentication (Diaz, Arroyo, & Rodriguez, 2011; Weippl, 2005), and passwords can be easily compromised (Levy & Ramim, 2009). Because of these issues, any personal information contained within ELS is also at risk and must be secured (Weippl, 2005).

Habit has also been found to impact user behavior (Limayem, Hirt, & Cheung, 2007; Verplanken, Myrbakk, & Rudi, 2005). Limayem et al. (2007) defined habit as "the extent to which people tend to perform behaviors (use IS) automatically because of learning" (p. 709). According to Verplanken and Aarts (2006), habits are "learned sequences of acts that have become automatic responses to specific cues, and are functional in obtaining certain goals or end-states" (p. 104). Habits occur without awareness or thought (Bargh, 1994; Nosek, Hawkins, & Frazier, 2011), and may be guided by implicit attitudes and triggers in the environment, rather than by conscious thought (Verplanken et al., 2005). Limayem et al. (2007) recommended additional research designed to improve understanding of the influence habit has on users' IS practices.

Fogel and Nehmad (2009) suggested that risky online information sharing practices continue to be problematic, and found that individuals who had a profile on a SNS had greater risk taking attitudes than individuals who did not. In a recent survey of 1,002 young adults between the ages of 18-24, risky online PISP increased the risks to the respondents' personal information (WSJ, 2010). About 73% of the respondents acknowledged they were concerned about being a victim of online fraud or identity theft, and 64% claimed to have experienced some form of unauthorized use of their personal

information. Despite this, 71% reported that they are not always as careful as they should be when it comes to sharing their personal information online (WSJ, 2010). Therefore, additional research on users' PISA, PISH, and PISP within SNS and ELS is warranted (Dinev & Hart, 2006; Furnell, 2008; Levy & Ramim, 2009; Power & Trope, 2006).

Dissertation Goal

The main goal of this study was to assess the influence of users' PISA on PISH and PISP, as well as compare the three constructs between SNS and ELS. According to Furnell et al. (2008), "users have significant issues with their online behavior, carrying out risky online practices" (p. 235). Therefore, this study compared users' awareness of information security threats related to their online sharing of personal information, and their PISP, while comparing it between SNS and ELS. This study also posited that, even though users may be aware of the risks to their personal information, habit may also influence their information sharing practices, thus, potentially placing their personal information at risk. Therefore, this study also compared users' habits regarding their personal information sharing within SNS and ELS.

The need for this work is demonstrated by the work of Furnell et al. (2008), Dinev and Hart (2006), Norberg, Horne, and Horne (2007), as well as Levy and Ramim (2009), who found that, although users are generally aware about the threats to their personal information they face while using online resources, their online PISP often do not follow their level of awareness or concern. According to Furnell et al. (2007), even those users who consider themselves to be advanced users demonstrate deficiencies in awareness of the threats that exist to their personal information. The need for this work is

also supported by Furnell (2008), who stated that "although a new generation of 'digital natives' is emerging that are more IT-literate, this by no means implies that they will be more naturally security-aware" (p. 9). Furnell (2010) suggested that these, mainly young, users are enthusiastic and capable, but they share personal information with little caution or restriction. Furnell (2010) referred to these users as the "Generation wh(Y) bother?" (p. 11).

Even those who have experienced identity theft first-hand seem to think that security of personal information is not their responsibility (Furnell et al., 2008). Many believe they are not responsible for providing more than minimal protections, and that it is others' responsibility to protect their information (Furnell et al., 2007; Furnell, 2010). Results from a survey of 378 home PC users who had an Internet connection, McAfee and the National Cyber Security Alliance (NCSA) (2007) indicated that 98% of the respondents were aware of the importance of keeping computer security software up to date; however, only 52% actually had anti-virus software that had been updated within the last week. Moreover, the survey found that 26% of Americans who were 45 years and older had their security software, such as firewalls, anti-virus, and anti-spyware, enabled and up to date, compared to only 20% of those who were younger than 45 (McAfee/NCSA, 2007). As age and gender have been shown to influence the information sharing practices of users within SNS and ELS, this study used age and gender as covariates, in order to ensure the validity of the study. Users' prior exposure to identity theft was also investigated, with respondents indicating if they or someone in their family has personally been a victim of identity theft or other unauthorized use of their personal information.

Furnell (2008) suggested that the general state of user awareness is not encouraging, and recommended additional research into the security awareness and practices of users. The need for further investigation of user habits is demonstrated by Limayem et al. (2007), who suggested that user behavior is complex, and recommended additional research to help better understand the relationship between habit and practices. Because of the apparent contradiction between users' PISA, PISH, and PISP, as well as the increasing popularity of major IS tools such as SNS and ELS, additional research in both of these technology systems is recommended (Dinev & Hart, 2006; Furnell, 2008; Kritzinger & von Solms, 2006; Levy, 2007). The main research question this study addressed was: What is the difference between users' PISA, PISH, and PISP within SNS and ELS?

Hypotheses

The specific hypotheses this study addressed are:

H1a: There will be no statistically significant effect of SNS users' PISA on their PISP.

H1b: There will be no statistically significant effect of ELS users' PISA on their PISP.

H2a: There will be no statistically significant effect of SNS users' PISA on their PISH.

H2b: There will be no statistically significant effect of ELS users' PISA on their PISH.

H3a: There will be no statistically significant effect of SNS users' PISH on their PISP.

H3b: There will be no statistically significant effect of ELS users' PISH on their PISP.

H4a: There will be no statistically significant difference between users' PISA within SNS and users' PISA within ELS, when controlling for gender.

H4b: There will be no statistically significant difference between users' PISA within SNS and users' PISA within ELS, when controlling for age.

H5a: There will be no statistically significant difference between users' PISH within SNS and users' PISH within ELS, when controlling for gender.

H5b: There will be no statistically significant difference between users' PISH within SNS and users' PISH within ELS, when controlling for age.

H6a: There will be no statistically significant difference between users' PISP within SNS and users' PISP within ELS, when controlling for gender.

H6b: There will be no statistically significant difference between users' PISP within SNS and users' PISP within ELS, when controlling for age.

Figure 1 presents the conceptual map for this research.

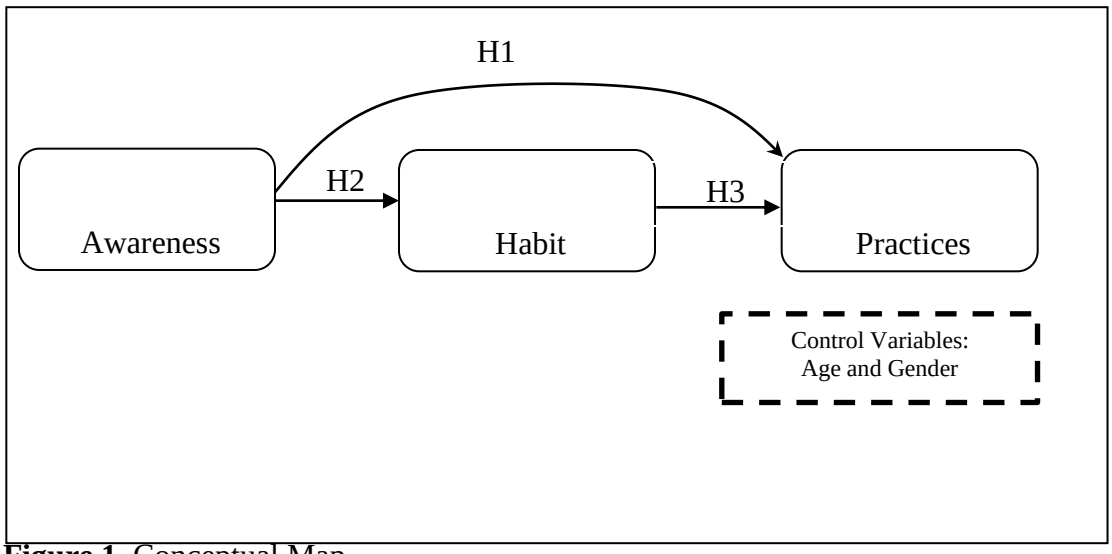

Figure 1. Conceptual Map.

Relevance

This study is relevant, as it sought to facilitate a better understanding of users' PISA, PISH, and PISP within SNS and ELS. According to Shaw et al. (2009), information security and the protection of personal information continue to be a problem. There has been a variety of research studies focused on the issues relating to identity theft (Anderson et al., 2008; Furnell et al., 2007). However, a review of the literature revealed few studies that have focused on personal information security as it relates to ELS (El-Khatib, Korba, Xu, & Yee, 2003; Kritzinger & von Solms, 2006; Webber, Lima, Casa, & Ribeiro, 2007). According to Furnell (2008), security issues have been largely ignored in SNS, as well. As users share an ever increasing amount of personal information within these systems, understanding users' PISA, PISH, and PISP is critical to securing the personal information stored in these systems.

Significance

This research is significant, as it advanced current research in computer security and facilitated an increase in the body of knowledge regarding IS users' behavior as it relates to their awareness, habits, and practices in the context of personal information sharing. According to Hazari, Hargrave, and Clenney, (2008) understanding users' behavior is a critical factor in information security awareness. As risky information sharing practices have been related to increased security incidents such as identity theft, insights into users' PISA, PISH, and PISP can potentially help to reduce these IS security threats by identifying where educational, managerial, and policy decisions should be focused (Furnell et al., 2007).

Barriers and Issues

One barrier to this research was in the difficulty with the definition of information security awareness. The expert panel was comprised of 10 IS faculty member who are experts in the IS field, each of which may have had his or her own ideas as to how to define information security awareness. To mitigate this problem, the researcher provided the members of the expert panel with enough background to understand this difficulty and the definition of PISA, and explained the purpose of the research and how the items were developed.

Limitations

A limitation of this study is related to the self-report method of measuring PISH. According to Verplanken and Orbell (2003), self-reporting of behaviors that are automatic present some limitations, as episodic behaviors or behaviors that are not clearly defined can be difficult to recall. Respondents may also be vulnerable to the tendency to want to provide consistent or socially-acceptable answers. The design of the SRHI helped limit this problem through the use of a validated, multiple-item instrument, rather than a single-item instrument (Verplanken & Orbell, 2003). The SRHI also breaks the concept of habit down into components that seem relatively easy to reflect on, which, according to Verplanken and Orbell (2003), may provide a valid and reliable way of measuring habit strength.

This study was conducted at a small private university in the southeastern United States. The university has approximately 3,000 undergraduate and graduate students. The

university offers 11 associate degrees, 12 bachelor's degrees, eight master's degrees, with 22 of the degrees offered completely online. It is a career-oriented, commuter university, with a student body of mainly working adults. Additional study will be required to replicate the findings within other institutions and within other populations.

Delimitations

This study limited the survey participants to a single, higher education university. The study also limited the ELS studied to a single ELS platform, Blackboard©, as well as a single SNS platform, Facebook©.

Definition of Terms

E-Learning System (ELS) – "the entire technological, organizational, and management system that facilitates and enables students learning via the Internet" (Levy & Murphy, 2002, p. 42).

Habit - "the extent to which people tend to perform behaviors (use IS) automatically because of learning" (Limayem et al., 2007, p. 709).

Habit – "learned sequences of acts that have become automatic responses to specific cues, and are functional in obtaining certain goals or end states" (Verplanken et al., 2005, p. 104).

Identity theft – "the unlawful use of another's personal identifying information" (Bellah, 2001, p. 222).

Information security – "the protection of personal data against accidental or intentional disclosure to unauthorized persons, or unauthorized modifications or destruction." (Udo, 2001, p. 165).

Information security awareness –"the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control" (Shaw et al., 2009, p. 92).

Personal information – names, addresses, demographic characteristics, lifestyle interests, shopping preferences, and purchase histories of identifiable individuals (Phelps, et al., 2000).

Personal Information Sharing Awareness (PISA) – "the degree of users' understanding about the security threats posed by the sharing of their personal information, and the awareness of their responsibilities and acts to exercise sufficient levels of information security control in order to protect their personal information" (Furnell, 2008; Shaw et al., 2009).

Personal Information Sharing Habits (PISH) – personal information sharing behaviors that are done automatically, and without awareness or thought (Verplanken et al., 2005; Limayem et al., 2007).

Personal Information Sharing Practices (PISP) – users' actual behaviors related to the sharing of individual-specific, personally identifiable information (Phelps et al., 2000).

Self-Report Habit Index (SRHI) – a 12-item index that provides a method of measuring the strength of habits, and does not simply measure the frequency of past and later behavior (Verplanken & Orbell, 2003).

Social Networking Sites (SNS) - Web-based services that allow individuals to 1) construct a public or semi-public profile within a bounded system, 2) articulate a list of other users with whom they share a connection, and 3) view and transverse their lists of connections and those made by others within the system (Boyd & Ellison, p. 211, 2007).

Summary

The purpose of chapter one was to introduce the study, identify the research problem, discuss and identify any barriers and limitations to conducting this study, and to provide a theoretical basis for this study. The research problem this study addressed is, although public awareness of the threat of identity theft has increased substantially, new avenues for identity fraud have contributed to an increasing number of security incidents, including identity theft. Valid literature supporting the need for this research was also presented.

Moreover, chapter one also presented the main goal, specific goals, and specific research questions that were addressed through this study. The main goal of this study was to assess the influence of users' personal information sharing awareness (PISA) on their personal information sharing habits (PISH) and the personal information sharing practices (PISP), as well as compare the three constructs between SNS and ELS. Prior literature that supports the main goal of this research was presented (Dinev & Hart, 2006; Furnell, 2008; Levy & Ramim, 2009; Power & Trope, 2006; Verplanken et al., 2005).

Chapter 2

Review of Literature

Introduction

In this chapter, a literature review was presented to review the relevant literature associated with the constructs: PISA, PISP, PISH, SNS, and ELS. According to Levy and Ellis (2006), "quality IS research literature from leading, peer-reviewed journals should serve as the major base of literature review as it provides sufficient theoretical background" for additional research (p. 185). This review provided an understanding about these areas, discovered what is already known about these constructs, and framed the hypotheses and research questions, thereby laying a solid foundation for this study.

Personal Information Sharing Awareness

According to Shaw et al. (2009), "information security awareness is becoming an important issue to anyone using the Internet" (p. 92). Users' lack of awareness of the threats posed by the sharing of their personal information increases the susceptibility of malicious attacks (Furnell, 2008; Kumar, Mohan, & Holowczak, 2008; Anderson et al. 2008). Information security awareness is regarded as not only users' general awareness of security issues and threats to their personal information, but also includes users' responsibilities in acting upon that awareness (Furnell, 2008; Rezgui & Marks, 2008; Shaw et al., 2009). Shaw et al. (2009) defined IS security awareness as "the degree of understanding of users about the importance of information security and their

responsibilities and acts to exercise sufficient levels of information security control to protect the organization's data and networks" (p. 92). Furnell (2008) categorized users as those who are merely aware and those who are properly aware. Users who are properly aware are those who have actually done something to protect their personal information. This study followed the example of Shaw et al. (2009) as well as Furnell (2008), and defined PISA as the degree of users' understanding about the security threats posed by the sharing of their personal information, and the awareness of their responsibilities and acts to exercise sufficient levels of information security control in order to protect their personal information.

This definition of PISA is supported in literature (Rezgui & Marks, 2008). Through a review of IS security awareness studies, Rezgui and Marks (2008) identified two categories of IS security awareness. The first category regards IS security awareness as "attracting users' attention to IS security issues" (p. 242), while studies in the second category regard IS security awareness as users' "understanding of IS security and, optimally, committing to it" (p. 242). McDaniel (1994) defined information security as "the concepts, techniques, technical measures, and administrative measures used to protect information assets" (p. l). Committing to IS security can be problematic, as many users are unaware of the proper configuration required for products such as Internet security suites, firewalls, and other technologies used to protect their personal information (Furnell, 2008; Kumar et al., 2008). Other users are simply unwilling or unable to configure the security devices (Furnell, 2008; Kumar et al., 2008). Therefore, although important, IS security cannot be accomplished by technical and procedural measures alone (Rezgui & Marks, 2008). Kumar et al. (2008) suggested that there is a

relationship between the two categories of awareness, with lack of awareness of security threats playing an important role in users' lack of adoption of the technological measures available to them. According to Rezgui and Marks (2008), educating all users to heighten their awareness of the threats posed by the sharing of personal information is required to accomplish effective information security.

In a study of 20 novice users, Furnell et al. (2008) investigated users' a) awareness of security threats, b) users' awareness and usage of security measures, c) attitudes toward security, d) practices of personal protection measures, and e) other factors that limit users' usage of online protection methods. Many of the respondents had personally experienced some form of security attack and were generally aware of the existence of threats to their personal information. Despite this, many of the respondents failed to use appropriate security protections for their systems. According to Furnell et al. (2008), the responses revealed "a lack of understanding of both the potential impact of the threats and the required scope of protection" (p. 237). Results also indicated that, although many users claimed to be aware of threats to their personal information, they often associated threats with specific activities such as online banking. Thus, security awareness was often context-specific and did not necessarily transfer to other contexts.

In another study of 32 attendees at an information security workshop, survey results revealed that the respondents continued to have a casual attitude regarding information security, even after the workshop (Furnell, 2008). According to Furnell (2008), many schools do not spend enough time on information security, and users are self-educating with very little success. Furnell (2008), also suggested that many users would turn to family or friends for assistance, as their knowledge of suitable sources for

information on how to protect their personal information is limited. Other than receiving advice from friends and the media, novice users have few resources from which to build awareness and knowledge regarding self-protections (Furnell et al., 2008). Tsohou, Spyros, Karyda, and Kiontouzis (2008) suggested that organizations are not implementing effective information security awareness training, either. According to Shaw, Keh, Haung, and Haung (2011), 55% of users stated that their security training was inadequate. Furnell (2008) suggested that a complete change in the method with which IS security awareness is promoted is needed. As the current approach of "build it and they will come" is ineffective and not working, Furnell et al. (2007) also suggested that more time should be spent raising IS users' awareness. IS users' inability to protect themselves and their resources could lead to the failure of the computing industry as a whole. According to Rezgui and Marks (2008) as well as Kumar et al. (2009), the number of studies that consider information security awareness in-depth is limited. Therefore, additional research into users' IS security awareness and the security threats caused by their sharing of personal information is warranted.

Table 1. Summary of PISA Studies

Study	**Methodology**	**Sample**	**Instrument/ Constructs**	**Main findings or contribution**
Anderson et al., 2008	Commentary			Additional information is needed in order to develop methods of limiting the number of attacks.
Furnell, 2008	Commentary			A change required in the method of promoting security awareness. Users more computer savvy, but not necessarily more security aware.

Table 1. Summary of PISA Studies (continued)

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Furnell et al., 2007	Empirical Survey	415 home users	Perceptions of security issues, attitudes towards the use of safeguards	There is clearly a lack of usable understanding among home users; home user environments are now at a greater risk than corporate networks.
Furnell et al., 2008	Empirical Survey	20 novice users	Awareness and experience of threats, awareness and usage of security measures, attitudes and practices towards protection online, factors that may limit protection from the individual's perspective	More time energy money and effort needs to be invested to raise computer security awareness.

Table 1. Summary of PISA Studies (continued)

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Kumar et al., 2008	Empirical Survey	130 students from a large public university	Awareness of security measures, Computer anxiety, Perceived ease of use, Perceived usefulness attitude, Intention to use firewall, Concerns for information privacy	Home user security awareness should be encouraged; developers and governments should make more of an effort to encourage, educate, and heighten home users' awareness.
McDaniel, 1994	Commentary			Dictionary defining computing technological terms
Rezgui & Marks, 2008	Case study			Factors such as conscientiousness, social conditions, cultural assumptions and beliefs affect university staff attitude towards information security awareness.
Shaw et al., 2009	Empirical Survey	154 freshmen in a MIS class	Perception, Projection Comprehension	Security awareness can be positively and negatively influenced by media richness. Moreover, hypermedia richness is the most effective approach to enhance security awareness.

Table 1. Summary of PISA Studies (continued)

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Shaw et al., 2011	Experimental	78 undergraduate students	Information security awareness	Knowledge maps improve learners' understanding toward target knowledge.
Tsohou et al., 2008	Literature review and analysis			The lack of clarity and definition in IS security awareness has led to the frustration of practitioners and managers.

Personal Information Sharing Practices

In spite of the increase in security problems related to the unauthorized use of personal information, there has not been a corresponding improvement in users' PISP (Anderson et al., 2008; Furnell et al., 2007). Even though users may be generally aware of security concerns and claim to engage in good practices, unawareness of the nature of the security risks to their personal information may lead to users' poor PISP (Acquisti & Gross, 2006; Furnell, 2008). Van Niekerk and Von Solms (2010) suggested that the effectiveness of a user's information security practices is related to the user's awareness of good information security practices. However, some have suggested that users are, in fact, aware of these security risks, and because of continuing information security attacks, have a lack of confidence in the amount, type, and security of their personal information stored on the Internet (Berendt, Günther, & Spiekermann, 2005; Zukowski & Brown 2007). This lack of confidence also impacts users' PISP. For example, in a study of 171 German Internet users, Berendt, Günther, and Spiekermann found that 75% of users were concerned about their personal information, with 60% of users reporting that they

avoided some Websites, and 47% of users reporting they sometimes provided false information.

Users have also reported sometimes refusing to provide information, or lying about their personal habits and preferences (Teltzrow & Kobsa, 2004). However, many users appear to have a complete lack of concern for their PISP (Furnell, 2008; Hart, 2008), which was demonstrated in studies related to users' password practices (Hart, 2008). Passwords have been, and will continue to be for the foreseeable future, the primary method of user authentication for most computer systems (Hart, 2008; Levy & Ramim, 2009). Results from a study of 36 students from a northeastern public university indicated that 80% of the respondents rarely changed their passwords (Hart, 2008). Moreover, 25% of the respondents revealed they had only lower case characters in their passwords, revealing a lack of concern for good password practices, as well as an attitude of indifference of the importance of good personal information security practices (Hart, 2008). According to Hart (2008) and Furnell et al. (2007), users neither care about good information sharing practices, nor do they want information regarding such practices. These beliefs contribute, in part, to poor PISP (Furnell et al., 2008).

According to Furnell (2008), poor personal information security practices are also evident within SNS, not only by the manner with which users post highly personal details about themselves, but also by how readily users invite others into their online social networks. Users' PISP on SNS such as Facebook© reveal their practices to be weak, with 87% of Facebook© users exposing personal information (Strater & Lipford, 2008). In a study of students at a large medical school in the southeast United States, 362 (44.5%) respondents had a Facebook© account (Thompson et al., 2008). Of the 362 respondents,

322 were medical students, while 40 were medical residents. Only 37.5% of Facebook© accounts were found to be private, and 31.7% of users revealed their area of residence, suggesting a large number of respondents had poor PISP. In another study of undergraduate students, 87.8% of respondents said they revealed their birthdate, 50.8% listed their addresses, 90.8% contained a picture of the profile owner, and 80% of the profiles included information that was personally identifiable (Gross & Acquisti, 2005). According to Lawler and Molluzo (2011), many users routinely share personal information in SNS, even when they are unaware of the data privacy practices of their SNS. In a recent study of 200 first year students, 14.4% of the respondents stated that their SNS profile was public, while 10.7% reported not knowing whether their profile was public or private (Lawler & Molluzo, 2011). Because of continuing problems with users' risky PISP, additional research regarding users' PISP is warranted (Furnell, 2008). Therefore, this study compared users' PISA, PISH, and PISP while using SNS and ELS.

Table 2. Summary of PISP Studies

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Acquisti & Gross, 2006	Empirical Survey & data mining	318 students at a college institution	Demographic differences, privacy concerns stated behaviors vs. actual behaviors	A majority of Facebook© users are aware of their profile settings. The study documented significant dichotomies between users' stated concerns and their actual behaviors.

Table 2. Summary of PISP Studies (continued)

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Anderson et al., 2008	Commentary			Additional information is needed in order to develop methods of limiting the number of attacks.
Berendt et al., 2005	Survey	206 Internet shoppers	Privacy concerns of users' practices	Users' state preferences on privacy, however, they do not act accordingly. Users' stated behaviors do not match their practices.
Furnell, 2008	Commentary			Recommended change in the method of promoting security awareness. Users are more computer savvy, but are not more security aware.
Furnell et al., 2007	Empirical Survey	415 home users		There is clearly a lack of usable understanding among home users; home user environments are now at a greater risk than corporate networks.

Table 2. Summary of PISP Studies (continued)

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Furnell et al., 2008	Empirical Survey	20 novice users	Awareness and experience of threats, awareness and usage of security measures, attitudes and practices towards protection online, factors that may limit protection from the individual's perspective	More time, energy, money, and effort need to be invested to raise computer security awareness.
Gross & Acquisti, 2005	Content analysis	4540 Undergraduate, graduate, faculty, and alumni	Online privacy, information revelation	A significant difference of activity exists on Facebook©® between genders. 80% of users' profiles contain useful identity information.
Hart, 2008	Empirical survey	123 students	Password practices and attitudes	Educating students regarding proper password usage had no effect; students did not want to learn about proper password usage.
Lawler & Molluzo, 2011	Empirical Survey	200 first year university students	Knowledge questions related to SNS privacy policies	Students do not read privacy policies and do not know how their information will be gathered, used, and shared. Privacy policies should be more easily accessible and easier to understand.

Table 2. Summary of PISP Studies (continued)

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Levy & Ramim, 2009	Empirical Survey	100 non-IT university students enrolled in e-learning courses	Code of Conduct Awareness, Perceived Ease of Use, Perceived Usefulness, Decision Making, Learners' Intention to Use Multi-biometrics	Perceived Usefulness has the most significant impact on learners' intention to use multibiometrics during e-learning exams; Ethical Decision Making demonstrated significant impact on intention to use multibiometrics.
Strater & Lipford, 2008	Interviews	18 undergraduate students	Examined Facebook© profiles and usage of privacy mechanisms	Mechanisms that provide awareness of the privacy impact of users' daily interactions are needed.
Teltzrow & Kobsa, 2004	Comparative	Data from 30 different online consumer surveys	User adaptive systems, personalization, privacy	The choice of personalization of systems or remaining anonymous with regard to personalization was not specified in this paper. However, neither will completely alleviate users' privacy concerns, which lead to a lack of trust.

Table 2. Summary of PISP Studies (continued)

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Thompson et al., 2008	Qualitative Analysis	813 medical students at the University of Florida	Networking use, norms of professionalism	Approximately half the students had a Facebook©® account that was publically available. A majority of the accounts had at least one piece of personally identifying publically shared information.
Van Niekerk & Von Solms, 2010	Commentary		Scheins model, information security culture, organizational culture	The paper suggests an addition of a fourth layer to Schein's corporate model could result in an effective information security culture.
Zukowski & Brown, 2007	Empirical survey	199 Internet users	Demographic factors, Internet users' concerns for information privacy	It was found that age, education, and income level influence Internet users' concern for information privacy, while gender and experience were found to have no influence.

Personal Information Sharing Habits

Habit has also been found to impact the behavior of IS users (Limayem & Cheung, 2008), including their PISP (Power & Trope, 2006). Habit has been studied alongside a variety of constructs, including behavioral intention (Lankton, Wilson, & Mao, 2010; Limayem et al., 2007) and IS usage (Yeh, 2009; Limayem et al., 2007; Limayem & Hirt, 2003; Gefen, 2003). Habit has been found to impact behavior over and above other factors (Burton-Jones & Hubona, 2006), and has been found to be a stronger

predictor of behavior than intention (de Bruijn, Kroeze, Oenema, & Brug, 2008; Kremers & Brug, 2008, Limayem, Hirt & Cheung, 2003). While habit has been studied significantly in other disciplines such as social science, a limited amount of research has been conducted regarding IS usage and habit (Limayem et. al, 2003; Limayem et. al, 2007; Ortiz de Guinea & Markus, 2009). Habit has been studied and is considered to be a significant construct in other disciplines, such as psychology, social psychology, health sciences, marketing, and organizational behavior (Limayem et. al, 2007; Ortiz de Guinea & Markus, 2009). In a study of 317 respondents, de Bruijn, Kremers, Singh, van den Putte, and van Mechelen (2009) investigated the effect habit had on the use of bicycles as an active means of transportation. de Bruijn et al. (2009) found habit strength was the strongest correlate of bicycle use, and was a stronger predictor of bicycle use than intention.

Limayem and Chueng (2008) studied the relationship between habit and IS use among 505 business students, and investigated how habit impacted the users' intention to use IS within ELS. Results indicated that habit had an impact not only on users' intention to use IS, but also on their intention to continue to use IS. As users performed behaviors over time, these behaviors became more determined by habit, and less by other influences such as behavioral intention; therefore, these behaviors appear to be more critical in the context of information security practices and personal information sharing (Limayem & Hirt, 2003). A high level of IS habit actually weakened the users' strength of intention to predict users' continued use of IS over time (Limayem & Cheung, 2008).

Habit theory has been validated across many disciplines, including psychology, genetics, and economics, with very limited attention in IS (Clark, Sanders, Carlson,

Blanche, & Jackson, 2007; Limayem et al., 2007). Habit has often been studied as a psychological construct; it has also often been measured as a behavioral frequency, using measures of past and later behavior (Verplanken & Orbell, 2003). According to Verplanken and Orbell (2003), research results consistently find that past behavioral frequency is, indeed, a predictor of future behavior. However, they argued that habits are a psychological construct; mere estimates of behavioral frequency are inadequate and have no explanatory value. Moreover, according Ajzen (2002), not all repeated behaviors are habits and, therefore, measures of past behavior are inadequate in measuring habits. Lankton et al. (2010) stated, "researchers have often represented habit as a result of prior behavior, although habits are more than frequently repeated behaviors, which do not always form habits" (p. 300).

Limayem et al. (2007) suggested that habit involves features of automaticity, including lack of awareness and difficulty to control. To address this limitation, Verplanken and Orbell (2003) developed the Self-Report Habit Index (SRHI). The SRHI is a 12-item index that provides a method of measuring the strength of habits, and does not simply measure the frequency of past and later behavior. The SRHI does not ask about habit directly, as habits are, by their nature, automatic and not done with conscious thought. Instead, the SRHI breaks down habit into components that are easy for users to reflect upon, such as the repetitive nature of their behaviors, the difficulty in controlling their behaviors, and the awareness of their behaviors (Verplanken & Orbell, 2003).

Lankton et al. (2010) investigated the relationship between habit and prior IT use in a study of 371 undergraduate students at a major university in the southwest United States. Results indicated that prior IT use had a significant effect on habit. They also

found that IT habits were developed despite low levels of prior use, further validating the suggestion of Verplanken and Orbell (2003) that habit should not be viewed as a measure of frequency of use.

Verplanken and Orbell (2003) suggested that a well-designed measure of habit must meet two conditions. The measure should have a theoretically sound foundation, and should be a multiple item instrument. This is the foundation that Verplanken and Orbell (2003) used in ensuring that the SRHI was a valid and reliable measure of habit. They conducted four studies to test the validity and reliability of the SRHI. The first study included 93 undergraduate students and inspected the test-retest reliability of the instrument. The second study included 86 undergraduate students and used the response-frequency measure to examine convergent validity, by relating the SRHI as independent measure that evaluated the automatic quality of habit. The third study included 133 undergraduate students and provided additional convergent validity by investigating the correlation between the SRHI and behavioral frequency. Their test investigated whether the SRHI was able to distinguish habit strength with respect to three different behaviors that were found to vary in behavioral frequency. The fourth study included 76 undergraduate students and was used to determine if SRHI could distinguish between daily and weekly habits. All four studies resulted in measures that validated the SRHI as an effective instrument, and provided a valid alternative to measuring behavioral frequency as a determinant of habit.

Verplanken and Orbell (2003) recommended additional research to gain a clearer understanding of the effectiveness of the SRHI. Verplanken et al. (2005) suggested that repetitive choices made by habits have received very little attention in research and

recommended additional research on constructs such as habit and practices. This study will followed the example of Verplanken et al. (2005), as well as Limayem et al. (2007), and defined users' PISH as personal information sharing behaviors that are done automatically, and without consciousness or thought. Because of the increasing amount of personal information that users are able to post online, it is important to have a clear understanding of the habits and practices of users who engage in personal information sharing activities (Power & Trope, 2006). According to Gefen (2003), while behavioral intention is a rational outcome, habit influences behavioral intentions more than previously thought, and should be studied further. Gaw (2009) also suggested that users must perceive a benefit to changing their PISP before they will change their habits. "IT researchers have recently begun to explore habit, which may be due to the extent to which people use IT automatically because of learning" (Lankton et al., 2010, p. 300). According to Lankton et al. (2010), habit should be evaluated from the perspective of how habit affects specific uses. Therefore, this study investigated the influence of users' PISH on their PISA and PISP, in the context of both SNS and ELS.

Table 3. Summary of PISH Studies

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Ajzen, 2002	Literature review			Suggest the limits of reasoned action are not habitual, but rather the result of improper planning to complete the planned action.

Table 3. Summary of PISH Studies (continued)

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Burton-Jones & Hubona, 2006	Empirical survey	125 U.S. Government employees	Perceived ease-of-use, perceived usefulness	External variables could have direct effects on usage behavior above their indirect effects. Moreover, it was also determined that TAM is more consistently better at predicting frequency than volume of usage.
Clark et al., 2007	Literature review, commentary			By increasing the understanding that habit influences both positively and negatively, better approaches can be developed to understand human responses to behaviors.
de Bruijn et al., 2008	Self-administered Survey	764 Dutch adults	Habit strength ;Theory of Planned Behavior	Indicates that intention and behaviors may be dependent upon habit strength.
de Bruijn et al., 2009	Survey	317 Dutch adults	Habit strength; Theory of Planned Behavior	Habit strength is a moderator of intention.
Gaw, 2009	Survey, experimental	58 Undergraduate students from Princeton University	Secure habits, users' password practices and reuse	Adoption of more secure habits derives from the realization of the benefits associated with more secure password management and adoption.

Table 3. Summary of PISH Studies (continued)

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Gefen, 2003	Survey	179 graduate and undergraduate business students	TAM, habit, e-commerce	Habit played a major role in users' continued use of IT, and that while PU and PEOU were important factors habit explained a large portion of variance in users' continued use of a Website.
Kremers & Brug, 2008	Empirical Survey	419 primary school children in Amsterdam	Habit strength, behavior measures	The current study suggested that intentions have little to do with children's activity level. Habit played an important role regarding children's activities.
Lankton et al., 2010	Survey	371 Undergraduate students at a US university	Habit, continued IT use, satisfaction, group analysis, important, task complexity	Prior IT use had a significant effect on habit. However, contrary to other studies, habits were developed even when low prior IT use was involved. Moreover, satisfaction was found to be the most influential habit antecedent.
Limayem & Chueng, 2008	Survey	313 Business students	Information system continuance, satisfaction, prior behavior, habit, e-learning	Strength of intention to predict continuance is weakened by high levels of habit. Moreover, it was implied that intention cannot be regarded as the only predictor of behavior.
Limayem et al., 2007	Empirical survey	227 Undergraduate students at a Hong Kong University	IS continuance, habit, expectation-confirmation theory, satisfaction, adoption	Based on this study, it is assumed that intention is no longer the main driver of continued IS usage. Instead, habit has major moderating effect on IS continuance.

Table 3. Summary of PISH Studies (continued)

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Limayem & Hirt, 2003	Empirical survey	94 Graduate and Undergraduate students at a Hong Kong University	Habit, IS usage, TPB, Internet-Based communication tools, education	The influence of intention on usage decreases as the use becomes more habitual.
Ortiz de Guinea & Markus, 2009	Literature review		IT continuance, Habit, automatic behaviors, environmental triggers, intention, cognition, reasoned action	The contrasting theories of activity and practice theories should be pitted against classical IS continuance theories in rival proposition. This would add considerable depth and breadth to IS continuance theory.
Power & Trope, 2006	Literature review		Privacy, security, data management	Organizations need to examine and appreciate the risks inherent in their adoption of highly useful, but vulnerable, new technologies. They need to assess the risks and correct deficiencies more promptly when they adopt such technologies.

Table 3. Summary of PISH Studies (continued)

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Verplanken & Orbell, 2003	Empirical survey	398 Undergraduate students in the Netherlands	Habit, psychological construct, habit strength,	The self-report habit index (SRHI), is an effect practical measure of habit strength which will likely serve to further advance the development and theory of habit.
Verplanken et al., 2005	Empirical survey	98 students from university of Tromso, Norway	Self-reported frequency of past behavior, self-reported habit frequency, response frequency measure, Self-report habit index (SRHI)	Of the four measures, SRHI is the only measure that is able to distinguish behaviors at a granular level of daily and weekly activities. Moreover, habit measures can be compared on a practical aspect as well. Researchers should determine specifically what type of habit they wish to measure and use appropriate measures.
Yeh, 2009	Empirical survey	308 Graduate business students at a public university in the southern US	Technology acceptance model, perceived usefulness, efficiency, effectiveness, perceived information quality, system quality, habit	The IS use confirmation is able to predict most of the success measures with a high degree of accuracy.

Personal Information Sharing in Social Networking Sites

SNS are rapidly gaining the attention of academia, as well as industry (Boyd & Ellison, 2008; Skeels & Grudin, 2009; Sturgeon & Walker, 2009). SNS are not secure by design; this, in part, leads to a lack of awareness of security issues and failure to engage in good PISP (Acquisti & Gross, 2006). According to Barnes (2006), many people are

unconcerned with the amount and type of personal information they share on SNS, as well as the threats posed by the sharing of personal information. As a result, the types of personal information users frequently share on SNS can lead to security threats to their personal information (Barnes, 2006; Skeels & Grudin, 2009; Sturgeon & Walker, 2009).

According to Weippl (2005), SNS were first introduced in 1997, with the introduction of sixdegrees.com©. Sixdegrees.com© did not gain significant interest or favor, primarily due to the early historical release of the site (Weippl, 2005). The most commonly used SNS, Facebook© and LinkedIn®, first appeared on college and university campuses, and have spread rapidly since their introduction in 2003 (Skeels & Grudin, 2009; Boyd & Ellison, 2008). According to Skeels and Grudin (2009), much discussion regarding industry adoption of SNS is taking place. Skeels and Grudin (2009) examined the potential benefits of using SNS in the workplace. They indicated many of the same concerns that have slowed the adoption of SNS on college and university campuses are encountered in industry as well. Even though the use of SNS has gained wide acceptance among users, the adoption and use of SNS has caused significant concern within the work environment because of the mixing of professional and personal lives.

Many SNS provide methods for users to post sensitive personal information (Weippl, 2005). Personal information commonly shared in SNS includes information such as birth date, workplace information, addresses, phone numbers, place of birth, childhood schools, pets, and other personal information about oneself, family, and friends (Furnell, 2008). Phelps, Nowak, and Ferrell (2000) identified personal information such as names, addresses, demographic characteristics, lifestyle interests, shopping

preferences, and purchase histories of identifiable individuals as being of concern to users. According to Phelps et al. (2000), it is the increase in usage, renting, and sharing of this personal information that is of primary concern to users. Yet it is this type of information that users often voluntarily, routinely, and often carelessly divulge in SNS (Furnell, 2008).

Despite awareness of information security threats to their personal information, users are increasingly engaging in risky online PISP (Furnell, 2008; Norberg et al., 2007). Risky online PISP include revealing personal information inadvertently, revealing unnecessary personal information, not reading information privacy policies, not being conscious of Web and home computer information security settings, opening spam email, replying to email spammers, using the same password on multiple accounts, and other risky online practices (Furnell, 2008; Udo, 2001). For example, in a survey of 87 SNS users, Furnell (2008) found that 87% identified where they work or their education level, 84% identified their full date of birth, 78% identified their location, and 23% listed their phone numbers. Because of the increasing amount of personal information users are storing within SNS, additional research within SNS is warranted. Therefore, this study compared users' PISH and their PISP within SNS, and the effect of PISH on PISP.

Table 4. Summary of SNS Studies

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Acquisti & Gross, 2006	Empirical Survey & data mining	318 students at a college institution	Demographic differences, privacy concerns stated behaviors vs. actual behaviors	A majority of Facebook©® users are aware of their profile settings. The study documented significant dichotomies between users stated concerns and their actual behaviors.
Barnes, 2006	Literature review		Posting of personal information on SNS	Awareness at all levels of society to correct the problem of posting of personal information on SNS.
Boyd & Ellison, 2008	Literature Review			There is a limited understanding of who and in what circumstance users are using SNS. There are vast areas of research in this area. Ethnographic research still needs to be done.
Furnell, 2008	Literature review			Current methods of security awareness are ineffective and more channels need to be employed to spread the word about security awareness.
Norberg et al., 2007	Empirical survey and experimental (pretest-posttest)	23 part-time graduate and 68 undergraduate students at a university in the northeast US	Privacy paradox, individuals intentions vs. their actual disclosure of personal information	People are far more willing to disclose information than their intentions indicate.

Table 4. Summary of SNS Studies (continued)

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Phelps et al., 2000	Empirical survey	556 households	Types of personal information consumers are willing to provide; consumers beliefs regarding benefits of providing personal information; consumers beliefs about personal information tradeoffs	Type of personal information requested, consumers' ability to control dissemination of provided information, perceptions about marketers knowledge about their personal interests, attitudes about direct mail, previous name removal behavior.
Skeels & Grudin, 2009	Empirical Survey	430 Employees of a large international enterprise	Attitudes and behaviors associated with social networking software	SNS is used heavily throughout the organization studied in this research. However, it was discovered that tension exists between management and the use of SNS in the enterprise.
Sturgeon & Walker, 2009	Empirical Survey	147 students and faculty from a private mid-sized masters university in the United States	Opinions and reactions of faculty and students in reference to their use of Facebook©®	The study found that an indirect causal relationship between faculty use of SNS and student academic performance exists. Additional research is recommended.
Udo, 2001	Empirical survey	158 Online IT users	Investigate the privacy and security concerns of online IT users	The majority of respondents have serious security concerns while shopping on the Internet.

Table 4. Summary of SNS Studies (continued)

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Weippl, 2005	Commentary			Security in e-learning has not been studied in detail. Therefore, additional and substantial research needs to be conducted in all aspects of e-learning security.

Personal Information Sharing in E-learning

E-learning has become the learning modality of choice, both in business environments and in higher education (El-Khatib et al., 2003; Selim, 2007; Zhang, Zhao, Zhou & Nunamaker, 2004). Personal information about the learners is increasingly stored within ELS, and may include name, address, and email address, as well as other information such as education records, training logs, professional development records, life-long learning record, personal blogs, electronic portfolios (e-portfolios), and work and training experience (Weippl, 2005). El-Khatib et al. (2003) identified the following types of personal information commonly stored within ELS: 1) personal contact information, 2) learner relationships, 3) learner preferences, 4) learner performance, and 5) portfolios. Therefore, the need for security has become a fundamental requirement of ELS (Levy & Ramim, 2009; Ramim & Levy, 2006; Weippl, 2005).

Many users are turning to e-learning, as it facilitates the ability of the learner to learn at home, anytime, and anyplace (Gerkin, Taylor, & Weatherby, 2009). Moreover, e-learners have greater success when they are able to study at home using their home computers (Selim, 2007). Users of ELS face an increased risk to their personal information because they often learn outside of an organization that would normally have

some protections in place. This underscores the need for awareness of personal information security within ELS (Furnell et al., 2007).

ELS are becoming the most widely used method of course material delivery for education and training environments (Levy, 2008). ELS no longer are used solely to facilitate and support online course delivery, but are also increasingly used as complementary systems for traditional classroom-based training, as well (Zhang et al., 2004). According to Ruiz, Mintzer, and Leipzig (2006), many of the advantages of ELS include learning delivery, which increases the personalization of course content and learner activities. Moreover, Selim (2007) indicated the inclusion of ELS with traditionally based classroom deliveries helps reduce cost and improve quality. This expanded role of ELS has now enabled the sharing and storage of large amounts of personal information (Ruiz et al., 2006).

According to Dalsgaard (2006), although SNS were not created for educational purposes, they can be used to support e-learning activities. The success of ELS largely depends on the acceptance of users, as well as use of such systems (Ball & Levy, 2008; van Raaij & Schepers, 2008). As personal information is stored in ELS, mitigating information security threats in ELS may lead to greater acceptance of these systems (Ong, Lai, & Wang, 2004). Weippl (2005) suggested that the ability of ELS to protect users' personal information is a prerequisite to acceptance of such systems. However, information security within ELS has largely been ignored (El-Khatib et al., 2003; Kritzinger & von Solms, 2006; Webber et al., 2007). Moreover, most e-learning innovations have focused on course development and delivery, with little or no consideration to information security as required elements (Anwar, Greer, & Brooks,

2006; Ramim & Levy, 2006; Webber et al., 2007). According to Kritzinger (2006), "it is vital that all electronic educational resources … are properly protected against possible security threats" (p. 345). According to Webber et al. (2007), security is one of the most important considerations when developing and deploying ELS. Securing ELS continues to be a problem that needs to be addressed to protect user information (El-Khatib et al., 2003).

The same security considerations that are applied to all other forms of IS must also be applied to ELS (Ramim & Levy, 2006; Weippl, 2005). These security considerations include confidentiality, integrity, and availability (Weippl, 2005). Ramim and Levy (2006) as well as Weippl (2005), indicated many people consider the inclusion of security in ELS to be a complexity that lengthens the development process, and increases the cost of ELS development. Ramim and Levy (2006) consulted for an organization and later published a paper that demonstrated the ease with which the security of ELS was compromised. A lack of proper security policies and procedures, as well as a disgruntled employee, compromised the system, causing the disruption of service on several occasions.

Students and faculty members comprise the main users of ELS. Mazer, Murphy, and Simonds (2007) as well as Skeels and Grudin (2009) suggested that there is a difference in the information sharing practices of faculty members and students within both SNS and ELS. These differences may be due to various factors, including age and professional status. They suggested that SNS use may be related to age, and found that 54% of the people in the 20-25 age group were more likely to accept new friend requests than other age groups. Moreover, the use of SNS was exceptionally high for the youngest

age group and declined with age. Skeels and Grudin (2009) also found SNS use may also be related to professional status, and that users with established careers may be less likely to use certain types of SNS than others. They found that SNS were used more by students and young professionals, while faculty members were less likely to use SNS, especially once they achieved tenure. Faculty members and students have been found to be uneasy with the posting of personal information within the same SNS because of the blurring of social and professional relationships. These issues have slowed the adoption of social networking tools within ELS (Skeels & Grudin, 2009).

ELS were adopted quickly in the 1990s, by both industry and education, with varying degrees of success (Ferdousi & Levy, 2010; Hogarth & Dawson, 2008; Selim, 2007). Due to the rapid adoption of ELS and the singular focus on pedagogical delivery, most ELS are unsecure and vulnerable to personal information security breaches (El-Khatib et al., 2003; Kritzinger & von Solms, 2006; Webber et al., 2007). According to Skeels and Grudin (2009), research regarding SNS use within e-learning has primarily focused on student use; therefore, additional research into a broader user base is warranted. Sturgeon and Walker (2009) suggested that faculty member use of SNS may have a positive effect on academic performance. However, Sturgeon and Walker (2009) further suggested that a paradigm shift is required before faculty members would employ the use of SNS. Roblyer, McDaniel, Webb, Herman, and Witty (2010) suggested that the SNS trend is relatively new, and there is little research on its acceptance and use in education. Therefore, additional research into users' PISA, PISH, and PISP within ELS is warranted (Dinev & Hart, 2006; Furnell, 2008; Levy & Ramim, 2009; Power & Trope, 2006).

This research is relevant, as it sought to address known deficiencies in research regarding PISA, PISH, PISP, and SNS. According to Tsohou, Kokolakis, Karyda, and Kiountouzis (2008), information security awareness continues to be a problematic issue due to the lack of theoretical background. Moreover, there continues to be a lack of empirical data and research in this area (Tsohou et al., 2008). Additionally, this study provided research into SNS which, according to Boyd and Ellison (2008), still has lack of experimental or longitudinal studies. According to Limayem and Hirt (2003), Limayem et al. (2007), as well as Ortiz de Guinea and Markus (2009), a limited amount of research has been conducted regarding IS usage and habit. Therefore, this study is significant and provided data to several areas that are lacking empirical data.

Table 5. Summary of ELS Studies

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Anwar et al., 2006	Commentary		E-learning, anonymity, pseudonymity, identity, personalization, reputation	The proposal of an environment ELS iHelp which would address some of the privacy issues described in the paper.
Ball & Levy, 2008	Empirical survey	56 IS and non-IS college professors	Computer self-efficacy (CSE), computer anxiety (CA), experience with the use of technology (EUT)	CSE was a significant predictor for the use of emerging education technology in the classroom.
Boyd & Ellison, 2008	Literature review		History of social networking sites (SNS)	According to the authors for scholars to gain a understanding of who is using SNS and to what extent, extensive qualitative and quantitative research needs to be conducted.

Table 5. Summary of ELS Studies (continued)

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Dalsgaard, 2006	Commentary			Students' self-governed learning processes in e-learning would be enhanced with the inclusion of social networks.
Dinev & Hart, 2006	Empirical and Survey	369 undergraduate and graduate students at university in the Southeastern US	Perceived Internet privacy risk, Internet privacy concerns, Internet trust, personal Internet interest, willingness to provide personal information to transact on the Internet	Internet privacy concerns inhibit e-commerce transactions on the Internet; Internet trust and personal Internet interest can frequently outweigh privacy risk concerns in the decision to disclose personal information on the Internet.
El-Khatib et al., 2003	Commentary			Policy-based management systems should be set up for e-learning privacy and security.
Ferdousi & Levy, 2010	Empirical and Survey	124 instructors at a community college in the Southeast United States	Resistance to change, Computer Self-efficacy, Perceived value, and attitude toward e-learning systems	The study suggests that of the four constructs, resistance to change has the most significant impact when predicting intention to use
Furnell, 2008	Commentary			A change in the method of promoting security awareness. The approaching digital natives are not more security aware.

Table 5. Summary of ELS Studies (continued)

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Furnell et al., 2007	Empirical and Survey	415 home users	Perceptions of security issues, attitudes towards the use of safeguards	There is clearly a lacking of usable understanding among home users; home user environments are now at a greater risk than corporate networks.
Gerkin et al., 2009	Descriptive		Perceived learning, learning satisfaction	E-learning is an effective and satisfactory medium for nursing education programs.
Hogarth & Dawson, 2008	Literature review, Model Development			Researchers may want to employ multiple approaches when implementing e-learning systems
Kritzinger & von Solms, 2006	Commentary			Identified four pillars required to ensure information in e-learning is secure.
Levy, 2008	Empirical and Survey	209 graduate online students	Critical Value Factor, Activity Theory and Cognitive Value Theory	The researcher states that there are five critical value factors of online learning activities. The researcher further states that a difference exists between gender in perceived cognitive value in several areas of online learning activities.

Table 5. Summary of ELS Studies (continued)

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Levy & Ramim, 2009	Empirical and Survey	100 non-IT university students enrolled in e-learning courses	Code of Conduct Awareness, Perceived Ease of Use, Perceived Usefulness, Decision Making, Learners' Intention to Use Multi-biometrics	Perceived Usefulness has the most significant impact on learners' intention to use multibiometrics during e-learning exams; Ethical Decision Making demonstrated significant impact on intention to use multibiometrics.
Limayem & Hirt, 2003	Empirical and Survey	60 university students from Hong Kong	Habit, Intentions, Affect, Perceived consequences, Social factors, Facilitating conditions, Actual usage behavior,	The findings demonstrate the importance of understanding the conscious and unconscious factors in the research of IS usage behavior.
Limayem et al., 2007	Empirical survey	227 Undergraduate students at a Hong Kong University	IS continuance, habit, expectation-confirmation theory, satisfaction, adoption	Based on this study, it is assumed that intention is no longer the main driver of continued IS usage. Instead habit has a major moderating effect on IS continuance.
Mazer et al., 2007	Experimental	133 undergraduate students at a Midwestern university	High self-disclosure, Medium self-disclosure, Low self-disclosure	Students demonstrate a higher motivation and success rate in courses where faculty have a high self-disclose rate. Therefore, Facebook© is one tool faculty can use to improve student performance and participation.

Table 5. Summary of ELS Studies (continued)

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Ortiz de Guinea & Markus, 2009	Literature review		IT continuance, Habit, automatic behaviors, environmental triggers, intention, cognition, reasoned action	The contrasting theories of activity and practice theories should be pitted classical IS continuance theories in rival proposition. This would add considerable depth and breadth to IS continuance theory.
Power & Trope, 2006	Literature review		Privacy, security, data management	Organizations need to examine and appreciate the risks inherent in their adoption of highly useful, but vulnerable, new technologies They need to assess the risks and correct deficiencies more promptly when they adopt such technologies.
Ramim & Levy, 2006	Case study		E-learning Security	E-learning is critical to the educational mission of all institutions and as such proper policy and procedures accompanied with well qualified and trained IT staff are required to ensure continued delivery of content in e-learning systems.

Table 5. Summary of ELS Studies (continued)

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Roblyer et al., 2010	Survey	182 faculty and students at a mid-sized Southern university	Comparison of faculty and student use of Facebook©	Students view Facebook© as a viable tool to increase face-to-face time with a professor. Unfortunately, this study does not indicate that professors view Face book with the same validity that students do.
Ruiz et al., 2006	Commentary			E-learning has a place in undergraduate, graduate, and continuing education in the medical field.
Selim, 2007	Survey	538 university students	E-learning Critical Success Factors	The study identified eight critical success factors for the adoption of e-learning by an institution of higher learning from a student perspective.
Skeels & Grudin, 2009	Empirical Survey	430 Employees of a large international enterprise	Attitudes and behaviors associated with social networking software	SNS is used heavily throughout the organization studied in this research. However, it was discovered that tension exists between management and the use of SNS in the enterprise.
Sturgeon & Walker, 2009	Empirical Survey	147 students and faculty from a private mid-sized masters university in the United States	Opinions and reactions of faculty and students in reference to their use of Facebook©	The study found that an indirect causal relationship between faculty use of SNS and student academic performance exists. Additional research is recommended.

Table 5. Summary of ELS Studies (continued)

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Tsohou et al., 2008	Literature review and analysis			The lack of clarity and definition in IS security awareness has led to the frustration of practitioners and managers.
van Raaij & Schepers, 2008	Empirical Survey	45 participants in an executive Chinese MBA program	Social Norms, Personal Innovativeness in the Domain of IT, Computer Anxiety, Perceived Usefulness, Perceived Ease of Use, System Usage	E-learning system designers should not only concern themselves with basic system design, but should also include the virtual learning environment to include individual differences.
Webber et al., 2007	Commentary		E-learning, Multi-agent systems, Standards to improve the development of secure systems	The inclusion of PMA3 platform will allow the inclusion of security standards in e-learning environments.
Weippl, 2005	Commentary			Security in e-learning has not been studied in detail. Therefore, additional and substantial research needs to be conducted in all aspects of e-learning security.
Zhang et al., 2004	Commentary			E-learning is an indispensable part of academia and professional training and as such we must continue to research and explore how to make e-learning more appealing and beneficial to all.

Summary of What is Known and Unknown in Research Literature

In this chapter, a review of literature was conducted that examined what is known about PISA (Furnell, 2008; Kumar et al., 2008; Anderson et al., 2008). Research results suggest that users' lack of awareness of the threats posed by the sharing of their personal information increases the susceptibility of malicious attacks (Furnell, 2008; Kumar et al., 2008; Anderson et al. 2008). Furnell et al. (2007) suggested that more time should be spent raising IS users' awareness; however, it is unclear as to how effective IS security awareness training has been, and how it should be approached (Furnell, 2008). According to Rezgui and Marks (2008) as well as Kumar et al. (2008), the number of studies that consider information security awareness in-depth is limited. With the increase in risky PISA, especially within SNS and ELS environments, this literature review also provided the foundation for the development of an instrument designed to investigate users' PISA.

Literature was also reviewed regarding users' PISP, which according to Furnell (2008), continues to be poor, with users increasingly participating in risky online personal information sharing. This demonstrates the need for additional research regarding factors that may be important in influencing users' PISP. One of the factors identified through the literature search is habit, which, according to Limayem and Cheung (2008) has been found to impact the behavior of IS users. However, while habit has been studied at length in other disciplines and is considered to be a major construct, few studies have been conducted in the IS discipline. This study built on the recommendation of Lankton et al. (2010), who recommended that habit should be evaluated regarding how it affects users within specific contexts.

Two environments identified where users demonstrate increasingly risky personal information sharing is within SNS and ELS. Users have already been found to participate in risky personal information sharing within SLS. According to Boyd and Ellison (2008), Skeels and Grudin (2009), as well as Sturgeon and Walker (2009), SNS are rapidly gaining the attention and use of academia. Therefore, a literature search was conducted that examined the personal information sharing within these environments. According to El-khatib et al. (2003), Selim (2007), and Zhang et al. (2004) e-learning has become the learning modality of choice in both business and higher education environments. Users also store much of the same type of information within ELS as that which they store in SNS. Therefore, the literature review provided the foundation for investigating the influence of users' PISH on their PISP within the contexts of SNS and ELS. It was also used to determine if, and to what extent, any differences may existed between users' PISA, PISH, and PISP within SNS and ELS.

Contributions of this Study

The main contribution of this study is to advance the understanding of users' awareness of information security threats, their personal information sharing habits, and their personal information sharing practices. Information gained from this study may help organizations in the development of better approaches to the securing of users' personal information, success in these areas including security, awareness training programs, and policy development may lead to a reduction in the occurrence of identity theft.

Chapter 3

Methodology

This study was a descriptive study, as it describes the differences in users' PISA, PISH, and PISP within SNS and ELS. The study used a survey methodology, and collected data through a Web-enabled survey instrument administered to students and faculty members.

The main research question this study addressed was: What is the difference between users' PISA, PISH, and PISP within SNS and ELS?

	Personal Information Sharing Awareness (PISA)	Personal Information Sharing Habits (PISH)	Personal Information Sharing Practices (PISP)
E-Learning Systems (ELS)			
Social Networking Sites (SNS)			

Figure 2. Research Design

The specific hypotheses this study addressed are:

H1a: There will be no statistically significant effect of SNS users' PISA on their PISP.

H1b: There will be no statistically significant effect of ELS users' PISA on their PISP.

H2a: There will be no statistically significant effect of SNS users' PISA on their PISH.

H2b: There will be no statistically significant effect of ELS users' PISA on their PISH.

H3a: There will be no statistically significant effect of SNS users' PISH on their PISP.

H3b: There will be no statistically significant effect of ELS users' PISH on their PISP.

H4a: There will be no statistically significant difference between users' PISA within SNS and users' PISA within ELS, when controlling for gender.

H4b: There will be no statistically significant difference between users' PISA within SNS and users' PISA within ELS, when controlling for age.

H5a: There will be no statistically significant difference between users' PISH within SNS and users' PISH within ELS, when controlling for gender.

H5b: There will be no statistically significant difference between users' PISH within SNS and users' PISH within ELS, when controlling for age.

H6a: There will be no statistically significant difference between users' PISP within SNS and users' PISP within ELS, when controlling for gender.

H6b: There will be no statistically significant difference between users' PISP within SNS and users' PISP within ELS, when controlling for age.

Instrument Development

Personal Information Sharing Awareness Measure

This study measured users' PISA using four items that were identified from a search of previously validated research (Oceja, Ambrona, Lopéz-Pérez, Salgado, & Villegas, 2010). The four items were presented twice; one set focused on SNS, while the second set focused on ELS. The questions were adapted from three separate studies conducted by Oceja et al. (2010). According to Oceja et al. (2010), although measuring awareness is a difficult task, awareness is measurable. As the specific PISA items were new, they were validated through an expert panel. PISA was measured using a five-point

Likert scale, where one indicated "Not at all" and five indicated "Extremely." The specific items numbered PISA1 through PISA4, are provided in Appendix A.

Personal Information Sharing Habits Measure

PISH was measured using the SRHI, which was developed and validated by Verplanken and Orbell (2003). The SRHI is a measure of habit strength, and was "developed on the basis of features of habit; that is, a history of repetition, automaticity (lack of control and awareness, efficiency), and expressing identity" (Verplanken & Orbell, 2003, p. 1313). They indicated the SRHI, which was designed to be adapted to different behaviors, demonstrated high internal and test-retest reliabilities, while it has been validated in additional studies (Verplanken & Melkevik, 2008).

Verplanken and Orbell (2003) originally developed and validated the SRHI through four separate studies. Verplanken and Orbell (2003) used a seven-point Likert scale for studies one and two, and an 11-point Likert scale for studies three and four. However, de Bruijn et al. (2009), de Bruijn et al. (2008), as well as de Bruijn and van den Putte (2009) adapted and validated the original scale to a five-point Likert scale. The five-point scale was found to be both valid and reliable, with a reliability measure using Cronbach's Alpha of .89 (de Bruijn & van den Putte, 2009). The research followed the example of de Bruijn and van den Putte (2009), and used a five-point Likert scale for measuring PISH. The specific items, numbered PISH1 through PISH12, are provided in Appendix A.

Personal Information Sharing Practices Measure

A review of valid literature was conducted to select the survey items for measuring PISP in SNS and ELS. Furnell (2008) developed a list of items as a pre-post

workshop survey that queried students regarding their PISP. A similar list was suggested by Anderson et al. (2008) and Furnell et al. (2007). The items selected are those that are commonly identified as items associated with, and leading to, identity theft (Anderson et al., 2008; Furnell et al., 2007). This study followed the example of Fogel and Nehmad (2009) and measured users' PISP within SNS and ELS using a Yes/No format. The specific items, numbered PISP1 through PISP12, are provided in Appendix A.

Expert Panel

According to Straub (1989), literature reviews and expert panels establish content validity. According to Sekaran (2003), content validity "establishes the representative sampling of a whole set of items that measures a concept, and reflects how well the dimensions and elements of the concept have been delineated" (p. 364). The four PISA items were developed through an extensive review of valid literature; however, the specific items on the survey instrument had yet to be validated in the context of SNS and ELS. Therefore, an expert panel was used in this research to ensure content validity of the four survey items. The expert panel consisted of IS faculty members and experts in the IS field. An anonymous survey was presented to the expert panel members, who were given one week to review and comment on the content of the instrument items. Once the panel submitted its recommendations, suggested changes were addressed in the final instrument.

Reliability and Validity

Reliability

Establishing reliability within research is the process of documenting internal consistency (Sekaran, 2003; Straub, 1989; Straub, Rai, & Klein, 2004). Straub et al. (2004) defined reliability as "the extent to which a variable or set of variables is consistent in what it is intended to measure" (p. 70). Cronbach's Alpha is the most commonly used measure to determine the reliability of an instrument (Hair, Anderson, Tatham, & Black, 1984; Sekaran, 2003; Straub et al., 2004). Cronbach's Alpha uses a scale that starts just above zero and goes to 1.0, with .60 being the lowest acceptable limited of the measure, and 1.0 nearing complete reliability (Gefen, Straub, & Boudreau, 2000). Nunnally (1967) first suggested that a Cronbach's score of .60 should be the lowest acceptable value of a reliable instrument. However, Nunnally (1967) as well as Nunnally and Bernstein (1994) suggested that .70 is the lowest limited deemed to be acceptable. Cronbach's Alpha was used on each set of construct items in the study to determine the reliability of each of the constructs. Additionally, Cronbach's Alpha if deleted' analysis was done for each set of construct items. The result of such analysis indicated which items provided a reduction in the overall constructs' Cronbach's Alpha; these were reviewed for rewording or possible removal from the construct item in further analyses.

Validity

Instrument validation is a crucial requirement of research (Straub, 1989). Historically, much of IS research has lacked validated instruments, calling into question the legitimacy of the results (Straub, 1989; Straub et al., 2004). Moreover, Straub et al.

(2004) suggested that IS research continues to have major hurdles to address in the development and validation of measurement instruments. Straub et al. (2004) defined valid measures as those that "represent the essence or content upon which the entity or construct is focused" (p. 5). According to Hair et al. (1984), validity is the measure of the extent to which an instrument measures what it is intended to measure. In the context of causal research, internal validity is the degree of confidence the researcher has (Sekaran, 2003). Additionally, Straub (1989) suggested that internal validity refers to "whether the observed effects could have been caused by or correlated with a set of unhypothesized and/or unmeasured variables" (p. 151). This study reduced the threat to validity by using PISH and PISP items that have been validated in prior research. An expert panel provided additional validity for the PISA items. External validity allows researchers to generalize the findings of investigations to other environments (Straub et al., 2004; Sekaran, 2003). This study was limited to one small private university in southeast United States. The university is a non-traditional commuter school with an average student age of 33 years. The respondents represented a true cross section of the population and provided a generalizable sample.

Population and Sample

This study was conducted at a small private university in Southwest Florida. According to Roscoe (1975), the rule of thumb for a sufficient sample size is between 30 and 500 participants. The total population for faculty in this study was approximately 125 faculty members, with approximately 50-60 faculty members expected to participate. A modest return of 10-15% from the approximate 2,800 in the student population was

expected to result in approximately 280-420 participants. Therefore, the sample size should be sufficient to ensure that the results are generalizable to the population. This study used a survey methodology to compare users' PISA, PISH, and PISP within SNS and ELS.

Pre-Analysis Data Screening

Pre-analysis data screening deals with the process of detecting and dealing with irregularities or problems with collected data (Levy, 2006). Pre-analysis data screening was performed to ensure consistency and accuracy of data. Data must be checked for accuracy and consistency to ensure the validity of the results (Mertler & Vanatta, 2010). According to Mertler and Vanatta (2010), there are four primary reasons to conduct pre-analysis data screening: 1) to ensure accuracy of the data collected; 2) to deal with the issue of response-set; 3) to deal with missing data; and 4) to deal with extreme cases, or outliers. Web based survey software was used to collect the data. According to Cooper and Schindler (2006), the use of Web-based survey software greatly enhances the quality of collected data and minimizes data inaccuracy issues. Web-based survey software automates the data handling process and, therefore, eliminates transcription errors, thus minimizing data entry irregularities.

Ensuring accuracy of the data includes ensuring that all responses are valid. Threats to the accuracy of the data were reduced by the Web-based delivery format of the survey, which limited item responses to only those that are valid. This eliminated common errors associated with collecting and recording responses using traditional, paper-based surveys. All items were set to be required, ensuring that there were no missing data. Response set, or response bias, is the tendency of respondents to agree with

questionnaire statements regardless of the content of the items, and is a potential threat to validity (Winkler, Kanouse, & Ware, 1982). Vague and confusing wording of survey items can lead to response bias. This threat was reduced in this study by using validated measures. All responses were also inspected, with potentially biased responses removed before final analysis. Extreme cases, or outliers, can result in serious distortion of results, and must be examined before final analysis of data (Hair et al., 1998). Mahalanobis Distance was used to determine if they should be retained or removed from the final analysis.

Data Analysis

Path analysis utilizes repeated applications of multiple regression to determine if a causal relationship exists between several variables (Mertler & Vannatta, 2010). This study followed the example of Shaw et al. (2009) and used path analysis to analyze hypotheses H1a through H3b to determine if a causal relationship existed between users' PISA, PISH, and PISP within the context of SNS and ELS. Moreover, the results were analyzed to determine if a predictive relationship existed between the variables (Shaw et al., 2009).

Analysis of covariance (ANCOVA) was used to compare two or more groups, while also being able to control for a variable that may exert an influence on the dependent variable (Mertler & Vannatta, 2010). According to Fogel and Nehmad (2009), age and gender are two variants that affect the online personal information sharing practices within SNS. Therefore, this research used ANCOVA to control for age and gender, and analyzed hypotheses H4a through H6b to determine if a difference exists between groups for PISA, PISH, and PISP within the context of SNS and ELS.

According to Fogel and Nehmad (2009), differences with regard to risky behaviors have been found between men and women, as well as among users of varying ages. Descriptive statistics are used to describe, the demographics of the participants in this study (Mertler & Vannatta, 2010). Therefore, this study followed the example of Fogel and Nehmad (2009) in using ANCOVA to describe and compare users' PISA, PISH, and PISP by gender and age.

Resources

Permission from the President of the University and the Executive Vice President of Academic Affairs was obtained to collect data from students and faculty members. Survey software was required to develop and deploy the survey instrument. eListen® was used for this purpose. Following data collection, Statistical Package for the Social Sciences® (SPSS) was used to analyze the data.

As human subjects were used in this study, IRB approval was also required to conduct this research, and was obtained prior to conducting the study. Respondents were assured that no personal data would be collected, and assured of total anonymity. They were also assured that their responses would be used in aggregate form only for the purpose of this research.

Summary

Chapter three discussed and identified the methodology and research design that were used in this study. This study is identified as a descriptive study as it sought to identify differences in users' PISA, PISH, and PISP within SNS and ELS. Additional

methods and items discussed in this chapter regarding this study include instrument development, reliability and validity, population and sample, pre-analysis data screening, and theoretical model development. As stated in chapter one, this study addressed 12 hypothesis statements.

The literature review provided the foundation for the development of the survey instrument to be used to measure PISA, PISH, and PISP in this study. The literature review revealed many difficulties with measuring PISA (Oceja et al. 2010). PISH was measured using the SRHI, which is a measure of habit strength that was developed and validated by Verplanken and Orbell (2003). PISP was measured using items selected from literature that are commonly identified as items associated with, and leading to, identity theft (Anderson et al., 2008; Furnell et al., 2007). Therefore, previously validated research was used to develop new items to measure users' PISA within the specific contexts of SLS and ELS in this study. In order to be validated, these items required the engagement of an expert panel.

The final survey instrument consisted of the following main parts: PISA, PISH, and PISP. Respondents were also asked to provide demographic information. As prior literature indicates that age and gender influence the information sharing practices of users within SNS and ELS, the study also used age and gender as covariates, in order to ensure the validity of the study. Users were also asked about their prior exposure to identity theft, with respondents indicating if they or someone in their family had personally been a victim of identity theft or other unauthorized use of their personal information. Respondents addressed PISA, PISH, and PISP with both SNS and ELS

environments. The specific SNS investigated was Facebook©; the specific ELS investigated was Blackboard©.

Chapter 4

Results

Overview

This chapter is organized similarly to chapter three, and details the data analysis of this study. The chapter describes the data collection process and the statistical methods used to analyze the data. First, details of the qualitative phase, via expert panel, are presented, which describe the process and recommendations of the expert panel. The results of the pre-analysis data screening follow the results of the quantitative phase. Next, the demographic data are presented, then the results of the reliability analysis. The chapter concludes with a summary of the data results and the procedures used during the analysis.

Expert Panel

An expert panel was conducted to confirm the validity of the survey instrument. An email was sent to 10 IS faculty members who are experts in the IS field. All 10 responded and provided feedback on the proposed survey instrument, providing a 100% response rate. Feedback from the experts included a recommendation to re-order some of the variables, and to place PISH and PISP before PISA. Members of the expert panel also suggested that the text of the Likert scale for PISA was not quite appropriate, and should be changed from not at all, slightly, moderately, very, and extremely, to never, seldom,

sometimes, often, and always. It was felt that this change in the wording of the scale would better reflect the action in question.

Quantitative Phase

The final revised survey instrument was converted to a Web-based survey format. An email invitation was emailed to 2,159 students and 221 faculty members. The email link contained the URL to the Web-based survey, which is shown in Appendix E. There were 298 student and 94 faculty member responses to the survey. This resulted in response rates of 13.9% for students and 42.9% for faculty members. Overall, the response rate was 16%. The data was collected during May of 2012.

Data Collection and Analysis

Pre-Analysis Data Screening

Before analysis, data were scrutinized for possible data irregularities. Pre-analysis data screening should be conducted for four reasons: (a) data accuracy, (b) issues with response sets, (c) missing data, (d) and to deal with extreme cases of outliers (Levy, 2006). Data accuracy was not found to be a problem, as the survey was designed to provide automated answers via radial buttons. Participants could also only select one answer per item. The data were collected and stored by the software; therefore, no manual manipulation or transposition of the data was required. This eliminated the need for a manual inspection for human error of data entry. To ensure that no respondent had selected the same response for every item, the data were visually inspected for response sets, and no response set issues were identified.

An analysis of the data was conducted to check for outliers. Outliers are responses with extreme values that could potentially unduly influence or skew the results of a solution or model (Mertler & Vanatta, 2010). Outliers were identified by conducting a Mahalanobis Distance analysis. Table 6 shows the result of the Mahalanobis Distance analysis. Case numbers 4 and 101 were identified for further examination due to their very high Mahalanobis distance value from the rest of the cases.

Table 6. Mahalanobis Distance Extreme Values

			Case Number	CaseID	Value
Mahalanobis Distance	Highest	***1***	***101***	***101***	***138.96709***
		2	***4***	***4***	***136.38766***
		3	387	391	131.79156
		4	188	188	130.73703
		5	358	362	129.74384
	Lowest	1	122	122	14.39576
		2	154	154	16.39328
		3	209	209	17.26820
		4	123	123	18.24029
		5	236	236	19.24998

An additional inspection of the Mahalanobis box plot shown in Figure 3 revealed that items 4 and 101 were extreme outliers. Therefore, items 4 and 101 were removed from the data set.

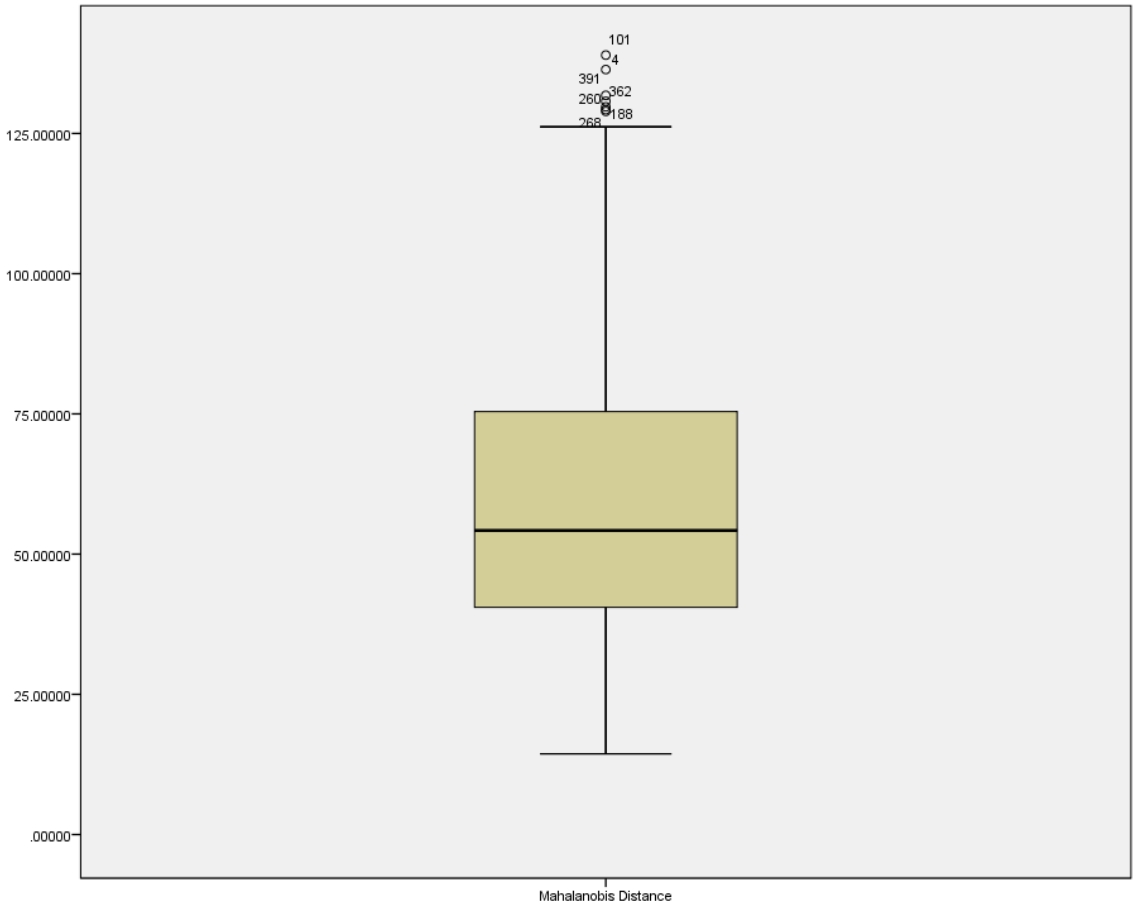

Figure 3. Mahalanobis Distance Box Plot

Reliability Analysis

The Cronbach's Alpha coefficient was then calculated for each variable to determine the reliability of the instrument. The PISA_E and PISA_S constructs possessed overall high reliability with scores of .89 and .877, respectively. Additionally, the Cronbach's Alpha "if item deleted" was calculated to determine if the reliability would be improved by removing any of the items. Analysis determined that all of the PISH_E items were reliable, with an overall reliability score of .913. However, PISH_S revealed that items PISH4S and PISH10S were problematic, as the reliability coefficients would be higher if those items were deleted. The coefficients for PISH4S and PISH10S were .911 and .912, respectively. After a review of the items PISH4S and PISH10S, it was

determined that the wording of the items might have been confusing and the two items were deleted. The final overall reliability score for PISH_S went from .908 to .947.

Demographic Analysis

Upon completion of the pre-analysis data screening, 390 respondents were usable, with 296 students and 94 faculty members. Of the student respondents, 201, or 68%, were female, while 95, or 32%, were male; additionally 53 female faculty members, 56%, and 41 male faculty members, 44%, completed the survey. The distribution of the data collected indicates that the age and gender of the sample appeared to be representative of the population of students and faculty members at the university. Table 7 displays the respondents by gender, age, marital status, and education level. Table 8 displays statistics for the number of years students and faculty members have used a computer. Table 9 displays statistics showing how many e-learning courses students and faculty members had previously taken.

Table 7. Respondents by Gender, Age, Marital Status, and Education Level

Item	**Frequency**	**Percentage**
Student Gender		
Male	95	32%
Female	201	68%
Faculty Gender		
Male	41	44%
Female	53	56%
Age of Students		
18 or under	3	1%
19-24	36	12%
25-29	53	18%
30-34	49	16%
35-39	37	13%
40-44	32	11%
45-54	59	20%
55-59	19	6%
60 or older	8	3%

Table 7. Respondents by Gender, Age, Marital Status, and Education Level (continued)

Item	Frequency	Percentage
Age of Faculty		
18 or under	0	0%
19-24	0	0%
25-29	6	6%
30-34	6	6%
35-39	4	4%
40-44	12	13%
45-54	27	29%
55-59	18	19%
60 or older	21	23%
Marital Status Student		
Married	158	53%
Single	88	30%
Divorced	48	16%
Separated	0	0%
Widowed	2	1%
Marital Status Faculty		
Married	64	68%
Single	15	16%
Divorced	12	13%
Separated	0	0%
Widowed	3	3%
Education Level Student		
Graduated from high school or GED	136	47%
Vocational or trade school	55	20%
Bachelor degree	69	23%
Post-graduate Diploma	11	1%
Master Degree	25	9%
Education Level Faculty		
Graduated from high school or GED	0	0%
Vocational or trade school	0	0%
Bachelor degree	10	11%
Post-graduate Diploma	52	55%
Master Degree	32	34%

1

Table 8. Respondents by Number of Years Using a Computer

	Minimum	Maximum	Mean	Std. Deviation
Number of Years using a Computer				
Students	0	40	17.9	7.03
Faculty	3	50	24.7	8.56

Table 9. Respondents by Number of E-learning Courses Taken

Students	Frequency	Percentage
1 E-learning course taken	53	18%
2 E-learning courses taken	26	9%
3 E-learning courses taken	36	12%
4 E-learning courses taken	41	14%
5 E-learning courses taken	19	6%
6 E-learning courses taken	59	20%
7 E-learning courses taken	61	21%
10 or more E-learning courses taken	1	.3%

Faculty	Frequency	Percentage
1-2 E-learning courses taken	14	15%
3 E-learning courses taken	6	6%
4 E-learning courses taken	5	5%
5 E-learning courses taken	9	9%
6 E-learning courses taken	11	11%
7 E-learning courses taken	49	52%

Path Analysis

Path analysis is used to estimate causal relations among several variables by utilizing multiple applications of multiple regression. In order to perform the path analysis, the aggregated values of the independent variables PISA_S and PISH_S were calculated and regressed against the aggregate value of the dependent variable PISP_S. Additionally, the aggregated values of the independent variables PISA_E and PISH_E were calculated and regressed against the aggregate value of the dependent variable

PISP_E. The results then were interpreted to determine if a causal relationship existed between the variables. This analysis addressed the following hypothesis statements:

H1a: There will be no statistically significant effect of SNS users' PISA on their PISP.

H1b: There will be no statistically significant effect of ELS users' PISA on their PISP.

H2a: There will be no statistically significant effect of SNS users' PISA on their PISH.

H2b: There will be no statistically significant effect of ELS users' PISA on their PISH.

H3a: There will be no statistically significant effect of SNS users' PISH on their PISP.

H3b: There will be no statistically significant effect of ELS users' PISH on their PISP.

In addressing the first hypothesis statements, the positive regression weight for PISA_S (.003) indicated that as PISA_S increased, PISP_S also slightly increased, however, this relationship was not significant at the .05 level (p=.805). The proportion of the variance in PISP_S that was explained by PISA_S, was R^2 = .0001. This addressed H1a: There will be no statistically significant effect of SNS users' PISA on their PISP. This hypothesis was not rejected, as analysis indicated that users' awareness of personal information sharing had no statistically significant effect on their personal information sharing practices in SNS. The coefficients and overall model are shown in Table 10.

Table 10. Variance in PISP_S Explained by PISA_S

Coefficients[a]

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	t	Sig.
1	(Constant)	.419	.042		10.070	.000
	Mean_AS	.003	.011	.013	.246	.805

a. Dependent Variable: Mean_PS

Table 10. Variance in PISP_S Explained by PISA_S (continued)

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.013[a]	.000	-.002	.24431

a. Predictors: (Constant), Mean_AS

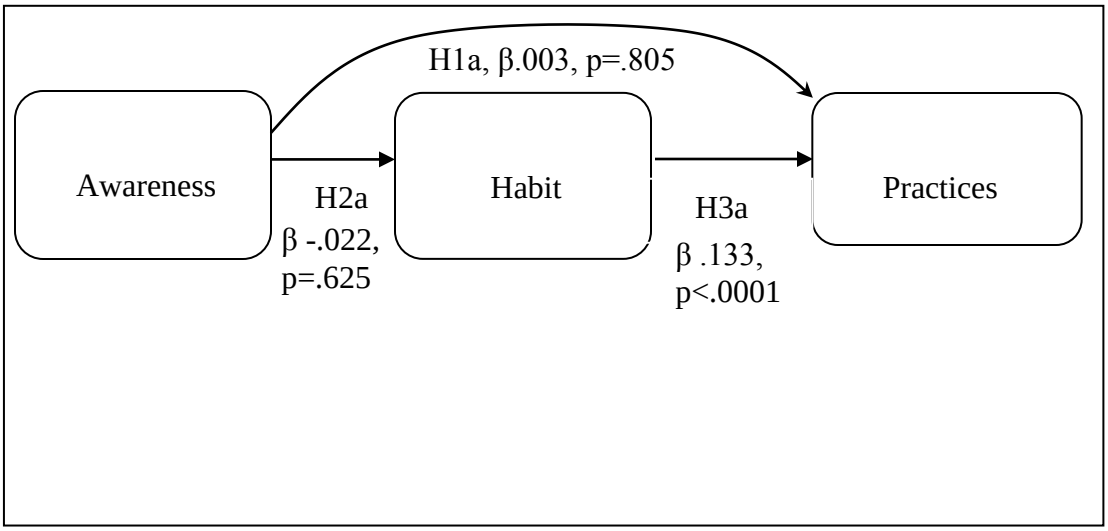

Figure 4. Conceptual Model for SNS

The negative regression weight for PISA_E (-.007) indicated that as PISA_E increased, PISP_E slightly decreased; however this relationship was not significant at the .05 level (p=.596). The proportion of the variance in PISP_E that was explained by PISA_E, was R^2=.001. This addressed H1b: There will be no statistically significant effect of ELS users' PISA on their PISP. This hypothesis was not rejected, as analysis indicated that users' awareness of personal information sharing had no statistically significant effect on their personal information sharing practices in ELS. The coefficients and overall model summary are shown in Table 11.

Table 11. Variance in PISP_E Explained by PISA_E

Coefficients[a]

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	t	Sig.
1	(Constant)	.444	.030		14.768	.000
	Mean_AE	-.007	.014	-.027	-.531	.596

a. Dependent Variable: Mean_PE

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.027[a]	.001	-.002	.24424

a. Predictors: (Constant), Mean_AE

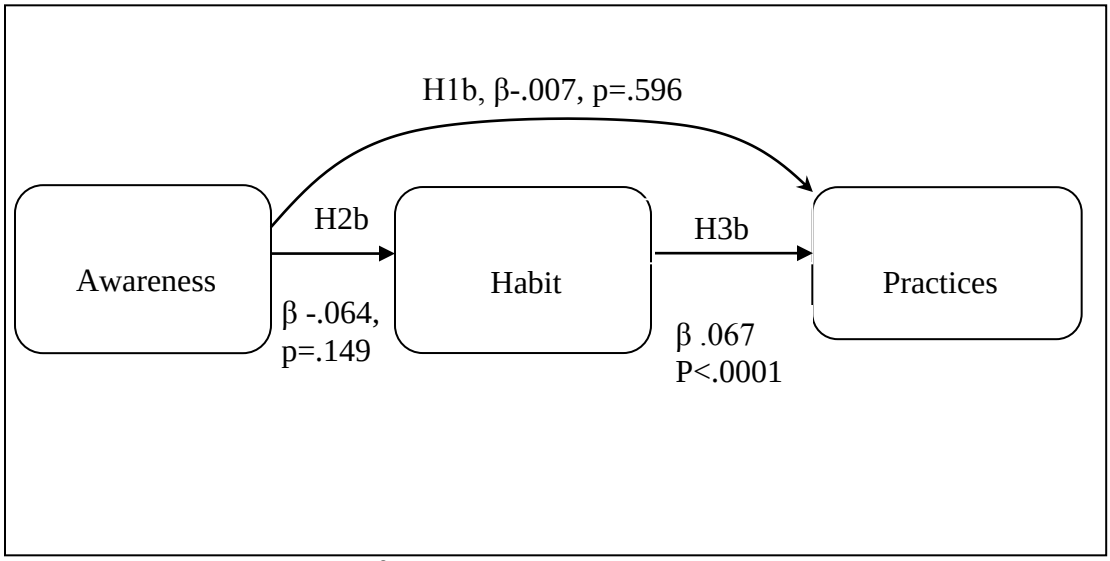

Figure 5. Conceptual Model for ELS

In addressing the second hypothesis statements, the negative regression weight for PISA_S (-.022) indicated that as PISA_S increased, PISH_S slightly decreased; however this relationship is not significant at the .05 level (p=.625). The proportion of the variance in PISH_S that was explained by PISA_S, was R^2 = .001, or one tenth of a percent. This addressed H2a: There will be no statistically significant effect of SNS users' PISA on their PISH. This hypothesis was not rejected, as analysis indicated that users' awareness

of personal information sharing had no statistically significant effect on their personal information sharing habits in SNS. The coefficients and model summary are shown in Table 12.

Table 12. Variance in PISH_S Explained by PISA_S

Coefficients[a]

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	t	Sig.
1	(Constant)	1.949	.163		11.956	.000
	Mean_AS	-.022	.045	-.025	-.490	.625

a. Dependent Variable: Mean_HS

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.025[a]	.001	-.002	.95657

a. Predictors: (Constant), Mean_AS

The positive regression weight for PISA_E (.064) indicated that as PISA_E increased, PISH_E also slightly increased, however, this relationship is not significant at the .05 level (p=.149). The proportion of the variance in PISH_E that was explained by PISA_E, was R^2 = .005. This addressed H2b: There will be no statistically significant effect of ELS users' PISA on their PISH. This hypothesis was not rejected, as analysis indicates that users' awareness of personal information sharing has no statistically significant effect on their personal information sharing habits in ELS. The coefficients and model summary are shown in Table 13.

Table 13. Variance in PISH_E Explained by PISA_E

Coefficients[a]

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	t	Sig.
1	(Constant)	1.780	.096		18.613	.000
	Mean_AE	.064	.044	.073	1.446	.149

a. Dependent Variable: Mean_HE

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.073[a]	.005	.003	.77741

a. Predictors: (Constant), Mean_AE

In addressing the third hypothesis statements, the positive regression weight for PISH_S (.133) indicated that as PISH_S increased, PISP_S also increased; this relationship was significant at the .05 level ($p<.0001$). The proportion of the variance in PISP_S that was explained by PISH_S, was $R^2 = .272$, or 27.2%. This addressed H3a: There will be no statistically significant effect of SNS users' PISH on their PISP. This hypothesis was rejected, as analysis indicated that users' personal information sharing habits within social networking environments had a statistically significant effect on their personal information sharing practices within SNS. The coefficients and overall model summary are shown in Table 14.

Table 14. Variance in PISP_S Explained by PISH_S

Coefficients[a]

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	t	Sig.
1	(Constant)	.179	.023		7.721	.000
	Mean_HS	.133	.011	.522	12.054	***.000****

a. Dependent Variable: Mean_PS

Table 14. Variance in PISP_S Explained by PISH_S (continued)

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.522[a]	.272	.271	.20840

a. Predictors: (Constant), Mean_HS

* - p<.0001

The positive regression weight for PISH_E (.066) indicated that as PISH_E increased, PISP_E also increased; this relationship was significant at the .05 level (p<.0001). The proportion of the variance in PISP_E that was explained by PISH_E, was R^2 = .045, or 4.5%. This addressed H3b: There will be no statistically significant effect of ELS users' PISH on their PISP. This hypothesis was rejected, as analysis indicated that users' personal information sharing habits in e-learning environments had a statistically significant effect on their personal information sharing practices in ELS. The coefficients and overall model summary are shown in Table 15.

Table 15. Variance in PISP_E Explained by PISH_E

Coefficients[a]

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	t	Sig.
1	(Constant)	.303	.032		9.451	.000
	Mean_HE	.066	.016	.212	4.271	***.000****

a. Dependent Variable: Mean_PE

* - p<.0001

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.212[a]	.045	.042	.23878

a. Predictors: (Constant), Mean_HE

Analysis of Covariance

Analysis of Covariance (ANCOVA) compares two or more groups, and controls for a variable (covariate) that may influence the compared groups. ANCOVA was used to determine if a difference exists between age and gender regarding PISA_S, PISA_E, PISH_S, PISH_E, PISP_S, and PISP_E. Prior to conducting the ANCOVA, the data was checked for normality. While the data was skewed slightly to the left, it was well within in normal research limits (Tabachnick & Fidell, 2007). The ANCOVA results are listed in the tables associated directly with the corresponding hypothesis statement.

To address the fourth hypothesis statements, ANCOVA was conducted to determine the difference between users' PISA_S and PISA_E, based on the covariate, gender. This addressed H4a: There will be no statistically significant difference between users' PISA within SNS and users' PISA within ELS, when controlling for gender. This hypothesis was not rejected, as analysis indicated that there was no statistically significant difference between users' PISA in SNS and PISA in ELS, based on gender. Table 16 indicates no significant difference existed between PISA_S and PISA_E when controlling for gender with $F(1, 388)=.293$, $n^2=.001$, $p=.589$ for the Mean_AS and $F(1, 388)=1.826$, $n^2=.005$, $p=.177$ for the Mean_AE.

Table 16. Difference in PISA by Gender between SNS and ELS

Tests of Between-Subjects Effects

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.
GENDER	Mean_AS	.345	1	.345	.293	.589
	Mean_AE	1.458	1	1.458	1.826	.177

a. R Squared = .001 (Adjusted R Squared = -.002)

b. R Squared = .005 (Adjusted R Squared = .002)

ANCOVA was conducted to determine the difference between users' PISA_S and PISA_E, based on the covariate, age. This addressed H4b: There will be no statistically significant difference between users' PISA within SNS and users' PISA within ELS, when controlling for age. This hypothesis was not rejected, as analysis indicated that there was no statistically significant difference between users' PISA in SNS and PISA in ELS, based on age. Table 17 indicates no significant difference existed between PISA_S and PISA_E when controlling for age with $F(1, 388)=3.37$, $n^2=.009$, $p=.067$ for the Mean_AS and $F(1, 388)=.020$, $n^2=<.001$, $p=.888$ for the Mean_AE.

Table 17. Difference in PISA by Age between SNS and ELS

Tests of Between-Subjects Effects

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.
AGE_GROUP	Mean_AS	3.941	1	3.941	3.366	.067
	Mean_AE	.016	1	.016	.020	.888

a. R Squared = .009 (Adjusted R Squared = .006)
b. R Squared = .000 (Adjusted R Squared = -.003)

To address the fifth hypothesis statements, ANCOVA was conducted to determine the difference between users' PISH_S and PISH_E, based on the covariate, gender. This addressed H5a: There will be no statistically significant difference between users' PISH within SNS and users' PISH within ELS, when controlling for gender. This hypothesis was partially rejected, as analysis indicated that there was no statistically significant difference in users' habits within ELS, when controlling for gender. However, there was a statistically significant difference in users' habits in SNS, when controlling for gender. Table 18 indicates that a difference does exist in PISH_S when controlling for gender, with $F(1, 388)=5.037$, $n^2=.013$, $p=.025$ for the Mean_HS . However, no

significant difference existed in PISH_E when controlling for gender, with F(1, 388)=.059, n^2=<.001, p=.809 for the Mean_HE.

Table 18. Difference in PISH by Gender between SNS and ELS

Tests of Between-Subjects Effects

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.
GENDER	Mean_HS	4.553	1	4.553	5.037	.025
	Mean_HE	.036	1	.036	.059	.809

a. R Squared = .013 (Adjusted R Squared = .010)
b. R Squared = .000 (Adjusted R Squared = -.002)

ANCOVA was conducted to determine the difference between users' PISH_S and PISH_E, based on the covariate, age. This addressed H5b: There will be no statistically significant difference between users' PISH within SNS and users' PISH within ELS, when controlling for age. This hypothesis was partially rejected, as analysis indicated that there was no statistically significant difference in users' habits within ELS, when controlling for age. However, there was a statistically significant difference in users' habits in SNS, when controlling for age. Table 19 indicates there was a significant difference based on age for PISH_S when controlling for age, with F(1, 388)=29.57, n^2=.071, p<.0001 for the Mean_HS. However, there was no significant difference for PISH_E when controlling for age, with F(1, 388)=.059, n^2=<.001, p=.591 for the Mean_HE.

Table 19. Difference in PISH by Age between SNS and ELS

Tests of Between-Subjects Effects

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.
AGE_GROUP	Mean_HS	25.157	1	25.157	29.570	.000
	Mean_HE	.176	1	.176	.290	.591

Table 19. Difference in PISH by Age between SNS and ELS

Tests of Between-Subjects Effects

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.
AGE_GROUP	Mean_HS	25.157	1	25.157	29.570	.000
	Mean_HE	.176	1	.176	.290	.591

a. R Squared = .071 (Adjusted R Squared = .068)

b. R Squared = .001 (Adjusted R Squared = -.002)

To address the sixth hypothesis statements, ANCOVA was conducted to determine the difference between users' PISP_S and PISP_E, based on the covariate, gender. This addressed H6a: There will be no statistically significant difference between users' PISP within SNS and users' PISP within ELS, when controlling for gender. This hypothesis was not rejected, as analysis indicated that there was no statistically significant difference between users' PISP in SNS and ELS, when controlling for gender. Table 20 indicates a marginally statistically significant difference existed by gender for PISP_S, with $F(1, 388)=3.77$, $n^2=.010$, $p=.053$ for the Mean_PS. A marginally statistically significant difference existed by gender for PISP_E with $F(1, 388)=3.77$, $n^2=.010$, $p=.053$ for the Mean_PE.

Table 20. Difference in PISP by Gender between SNS and ELS

Tests of Between-Subjects Effects

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.
GENDER	Mean_PS	.223	1	.223	3.774	.053
	Mean_PE	.223	1	.223	3.774	.053

a. R Squared = .010 (Adjusted R Squared = .007)

ANCOVA was conducted to determine the difference between users' PISP_S and PISP_E, based on the covariate, age. This addressed H6b: There will be no statistically

significant difference between users' PISP within SNS and users' PISP within ELS, when controlling for age. This hypothesis was rejected, as analysis indicated that there was a statistically significant difference between users' PISP in SNS and ELS, when controlling for age. Table 21 indicates age had a significant effect on PISP_S when controlling for age, with $F(1, 388)=29.87$, $n^2=.071$, $p<.001$. Age also had a statistically significant difference on PISP_E when controlling for age, with $F(1, 388)=29.87$, $n^2=<.071$, $p<.0001$ for the Mean_PE.

Table 21. Difference in PISP by Age between SNS and ELS

Tests of Between-Subjects Effects

Source	Dependent Variable	Type III Sum of Squares	Df	Mean Square	F	Sig.
AGE_GROUP	Mean_PS	1.656	1	1.656	29.868	.000
	Mean_PE	1.656	1	1.656	29.868	.000

a. R Squared = .071 (Adjusted R Squared = .069)

Identity Theft Victims

kAn analysis of the personal knowledge of and exposure to identity theft revealed that, of the 390 respondents, 169 or 43% has had a family member that had been a victim of identity theft. Additionally, 107 or 27% of the respondents of this study had also been victims of identity theft. Finally, 187 or 47% of the 390 respondents stated they knew of someone in their work place or school who had been a victim of identity theft.

Summary of Results

The purpose of this chapter was to provide results of the analysis performed and the results of the 12 hypothesis statements.

Table 22. Summary of Hypotheses

H1a: There will be no statistically significant effect of SNS users' PISA on their PISP.	Failed to reject
H1b: There will be no statistically significant effect of ELS users' PISA on their PISP.	Failed to reject
H2a: There will be no statistically significant effect of SNS users' PISA on their PISH.	Failed to reject
H2b: There will be no statistically significant effect of ELS users' PISA on their PISH.	Failed to reject
H3a: There will be no statistically significant effect of SNS users' PISH on their PISP.	Rejected
H3b: There will be no statistically significant effect of ELS users' PISH on their PISP.	Rejected
H4a: There will be no statistically significant difference between users' PISA within SNS and users' PISA within ELS, when controlling for gender.	Failed to reject
H4b: There will be no statistically significant difference between users' PISA within SNS and users' PISA within ELS, when controlling for age.	Failed to reject
H5a: There will be no statistically significant difference between users' PISH within SNS and users' PISH within ELS, when controlling for gender.	Partially rejected
H5b: There will be no statistically significant difference between users' PISH within SNS and users' PISH within ELS, when controlling for age.	Partially rejected
H6a: There will be no statistically significant difference between users' PISP within SNS and users' PISP within ELS, when controlling for gender.	Failed to reject
H6b: There will be no statistically significant difference between users' PISP within SNS and users' PISP within ELS, when controlling for age.	Rejected

This chapter presented the results of an empirical examination designed to describe the relationship and to determine the causal effect between PISA, PISH, and PISP within SNS and ELS environments. Prior to analyzing the data, pre-analysis data screening was performed to ensure the validity and accuracy of the collected data.

Cronbach's Alpha was performed on PISA, PISH, and PISP to determine how well the items were correlated to one another. The results of the Cronbach's Alpha demonstrated high reliability for all variables. Demographic data were requested from the survey participants in order to ensure the sample was representative of the population of the university. The distribution of the data appeared to be representative of the students and faculty at the university. The data appeared to be consistent with a normal distribution.

Two statistical analyses, path analysis and ANCOVA, were used to address the hypotheses presented in this study. Path analysis was used to determine if PISA and PISH had a statistically significant effect on PISP within the SNS and ELS environments. The results were mixed with respect to the hypothesis statements. H1a and H1b: As PISA_S increased, PISP_S also slightly increased; however it was found that this relationship was not significant. PISA_E demonstrated a negative regression weight, and that as PISA_E increased, PISP_E slightly decreased. This relationship was not significant. H2a and H2b: The negative regression weight for PISA_S indicated that as PISA_S increased, PISH_S slightly decreased. This relationship was found not to be significant. The positive regression weight for PISA_E indicated that as PISH_E increased, PISH_E also slightly increased. This was not significant. H3a and H3b: PISH_S indicated a positive regression weight which suggests that as PISH_S increased, PISP_S also increased. This relationship was found to be significant. PISH_E demonstrated a positive regression weight, which suggested that as PISH_E increased, PISP_E also increased. This relationship was found to be significant.

ANCOVA was used to determine if a difference exists regarding gender and age regarding PISA_S, PISA_E, PISH_S, PISH_E, PISP_S, and PISP_E. Once again, the

results were mixed. H4a and H4b: The variables PISA_S and PISA_E were not significant when controlling for gender or age. H5a and H5b: Gender did not have a significant effect on PISH_S and PISH_E. However, age was found to be statistically significant on both PISH_S and PISH_E. H6a and H6b: Gender had no effect on the variables PISP_S and PISP_E. However, age did have a statistically significant effect on PISP_S and PISP_E.

Summary

Chapter 4 reported results of the analysis performed in order to answer the 12 hypothesis statements proposed by this study. First, a literature review was conducted to investigate relevant research regarding PISA, PISH, and PISP. Feedback from an expert panel was used to develop the items on the survey and confirm the validity of the instrument. Once the final survey instrument was developed, it was administered to faculty members and students. A total of 2,159 students and 221 faculty members were surveyed, with 301 student and 95 faculty responses to the survey. This resulted in response rates of 13.9% for students and 42.9% for faculty. Of the student respondents, 201, or 68%, were female, while 95, or 32%, were male. Of the faculty respondents, 53, or 56%, were female, while 41, or 44%, were male. The overall response rate was approximately 16%, with the sample appearing to be normally distributed and representative of the population.

After completing pre-analysis screening, the data was examined for outliers, with 2 responses removed from the final data set, leaving 390 usable responses for further analysis. Next, the reliability of the instrument was verified through Cronbach's Alpha. Analysis indicated that two of the PISH items should be deleted. Once this was done, the

final Cronbach's Alpha coefficients were: PISA_E, .89; PISA_S, .877; PISH_E, .913; and PISH_S, .947.

This research supported H1a and H1b, and suggested that users' PISA had no significant effect on their PISP in either SNS or ELS. Results also supported Hypotheses H2a and H2b, and suggested that users' PISA also had no significant effect on their PISH in either SNS or ELS. However, hypotheses H3a and H3b were not supported, as PISH was found to have a significant effect on PISP, in both SNS and ELS. These results indicated that habit was the strongest indicator of users' practices.

Additionally, results indicated that there was no difference in users' PISA between the SNS and ELS environments, when controlling for age and gender. There was also no difference in users' PISH or PISP between SNS or ELS when controlling for gender. However, a difference did exist in users' PISH and PISP between SNS and ELS when controlling for age. The main finding of this research was the strong influence of users' PISH on PISP, which was stronger than the influence of users' PISA on PISP.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusions

This chapter begins with the conclusions drawn from the results of this study. The research question and hypotheses were outlined and reviewed, and implications for the study and contributions to the body of research were discussed. The chapter ends with recommendations for future research and a summary of this investigation.

The main goal of this study was to assess the influence of users' personal information sharing awareness (PISA) on their personal information sharing habits (PISH) and personal information sharing practices (PISP), as well as to compare the three constructs between SNS and ELS. This study addressed the 12 hypothesis statements proposed in this study, which were developed using a thorough review of related literature. The first hypotheses (H1a & H1b) were that users' PISA would have no statistically significant effect on their PISP. Findings from a path analysis on H1a and H1b suggested that this hypothesis was supported and that there was no significant effect of users' PISA on their PISP with respect to either environment – SNS or ELS. These findings were consistent with prior research suggesting that, although users are generally aware of information security threats to their personal information, they often continue to engage in risky online personal information sharing practices that may increase the risk of attacks on their personal information (Furnell, 2008).

The second hypotheses (H2a & H2b) were that users' PISA would have no statistically significant effect on their PISH. Findings from a path analysis on H2a and H2b suggested that this hypothesis was supported, and that there was no significant effect of users' PISA on their PISH with respect to either environment – SNS or ELS. This result is consistent with previous research suggesting that awareness did not impact habit (Limayem & Hirt, 2003). They are also consistent with the findings of Limayem and Cheung (2008), who suggested that as users performed behaviors over time, these behaviors became more determined by habit, and less by other influences.

The third hypotheses (H3a & H3b) were that users' PISH would have no statistically significant effect on their PISP. Findings from a path analysis on H3a and H3b suggested that this hypothesis was not supported and that there was a statistically significant effect of users' PISH on their PISP with respect to both environments – SNS and ELS. This finding is consistent with literature suggesting that habit had an effect on users' practices (Limayem & Chueng, 2008; Lankton et al., 2010). These findings also confirm the strength of habit found in prior studies, and are consistent with literature suggesting that behaviors may be dependent upon habit strength (de Bruijn et al., 2009). This is critical in the context of information security practices and personal information sharing.

The fourth hypothesis statements (H4a & H4b) were that there would be no statistically significant difference between users' PISA within SNS and ELS when controlling for gender and age. Findings from running ANCOVA on H4a and H4b determined that there was no statistically significant difference between users' PISA in either SNS or ELS environments, when controlling for gender or age. These findings are

consistent with prior studies that suggest that neither age nor gender had an effect on users' awareness (Dinev & Hart, 2006; Furnell, 2008; Levy & Ramim, 2009; Power & Trope, 2006).

The fifth hypothesis statements (H5a & H5b) were that there would be no statistically significant difference between users' PISH within SNS and ELS when controlling for gender and age. Results were mixed, as there was no statistically significant difference between users' PISH in ELS when controlling for gender and age. However, there was a statistically significant difference in PISH within SNS when controlling for gender and age. This finding is consistent with some literature, which suggested that age and gender had an effect on habit (Gaw, 2009; Kremers & Berg, 2008). However, other literature suggests that age and gender do not have an effect on habit (Burton-Jones & Hubona, 2006; Lankton, 2010; Yeh, 2009).

A review of the literature, also found mixed results regarding the influence of age and gender on habit. For example, in this study it was suggested that age and gender had no significant effect on PISH in ELS, however, they did on PISH in SNS. This could be due, in part, to the nature of the environments investigated. Results suggested that students trust that the institution is going to protect their personal information. This is illustrated in the results of the survey, which suggested that the respondents were less concerned with the information being shared by the institution than they were by the information being shared by the SNS provider.

The sixth hypotheses (H6a & H6b) were that there would be no statistically significant difference between users' PISP within SNS and ELS when controlling for gender and age. Results were mixed. Findings from running ANCOVA suggested that

there was no statistically significant difference in PISP in either SNS or ELS, when controlling for gender. This finding is consistent with literature that suggests that gender does not have an effect on users' practices (Dinev & Hart, 2006; Furnell, 2008; Levy & Ramim, 2009; Power & Trope, 2006). However, the results contradict Fogel and Nehmad (2009), who suggested gender does affect users' online personal information sharing practices. This contradiction may be simply due to the difference in age and gender of the participants in the two studies. The participants in this study were significantly older than those in the Fogel and Nemad (2009) study, with a greater percentage of females.

Results suggested that there was a statistically significant difference in PISP in both SNS and ELS, when controlling for age. This is consistent with the findings of Skeels and Grudin (2009), who found that SNS use declined with age. The results regarding age are also consistent with Fogel and Nehmad (2009), who suggested that age does affect users' online personal information sharing practices.

Respondents were asked if they had been, or knew of someone, either family or classmates, who had been a victim of identity theft. The results indicated that 43% had a family member who had been a victim of identity theft, 47% knew of someone who had been a victim of identity theft. Only 27% of the respondents in this study had personally been a victim of identity theft. This was significantly lower than had been reported in other research, where 64% claimed to have experienced some form of unauthorized use of their personal information (WSJ, 2010).

Implications

Implications for Practice

This research has several implications for practice. First, the results of this study can help organizations better understand users' awareness of the security risks their online sharing of personal information poses, and to review their security training programs in light of this understanding. However, the results of this study support the research of others that suggests awareness of personal information security risks and issues does not automatically translate into better personal information sharing practices. This is important for organizations to understand, as most traditional user security training programs target users' awareness of security issues and risks (Rezgui & Marks, 2008). This research can help organizations to better understand users' personal information sharing awareness and practices, and therefore, help them to develop more effective security policies, procedures, and security training programs.

Another implication for practice lies in the understanding of the influence of users' habits on their practices. Significant findings from this study confirm the research of others that habit has a strong influence on practices, and that once actions become habitual, they tend to occur without going through the cognitive planning process (Limayem et al., 2007; Cheung, 2008). Gaw (2009) suggested that understanding users' habits can help managers identify and manipulate habit formation. Organizations should design security awareness plans that encourage users to think about what personal information they post in online environments. These may include strategies to require users to pay attention to and actively process their awareness of security issues and their personal information sharing practices. This understanding can help managers to

integrate additional policies, procedures, and training into current training approaches designed to address users' habits and to promote the development of better habits regarding their personal information sharing practices.

Another implication for practice is in the area of the integration of SNS and ELS into the operations of organizations, and the related personal information sharing issues. As educational institutions and private organizations expand their usage of SNS and ELS, understanding users' awareness, habits, and practices regarding their sharing of personal information is critical to the securing of personal information within these environments. Areas for consideration include development of security policies and procedures regarding the sharing and protection of personal information; awareness programs designed to educate users about the risks of online personal information sharing and the organizations' use of personal information; and expansion of training programs designed to educate users regarding their online personal sharing habits and to promote development of better habits within these environments.

Implications for Research

The first implication for research is that this study provides the IS community a better understanding of users' PISA, PISH, and PISP within SNS and ELS. This study also provides the groundwork for the foundation of understanding the role of habit in relation to PISP, since few studies regarding habit in relation to IS research have been conducted (Hazari et al., 2008). This continues the recent trend of habit research toward research in IT that distinguishes habit from prior behavior frequencies (de Bruijn et al., 2008; Lankton et al., 2010; Limayem & Chueng, 2008).

Another important implication is that that this study provides the framework for additional studies regarding personal information security within ELS environments. According to El-Khatib et al. (2003), Kritzinger and von Solms (2006), as well as Webber et al. (2007), personal information security within ELS has been largely ignored. Furnell (2008) further suggests that the study of IS issues with respect to SNS has also been ignored. This study provides a framework for additional studies regarding personal information security within the SNS and ELS environments.

According to Hazari et al. (2008) there is a need to better understand the PISA of users. This study provides a basis for gaining a better understanding of how PISA, PISH, and PISP interact to influence users' online sharing of personal information. The results of this study will help guide researchers as they seek methods of improving users' personal information sharing awareness and practices. This study clearly suggests that habit is the strongest contributor to users' information sharing activities. According to Clark et al. (2007), understanding habit will better help researchers understand behavioral responses. Additional research is recommended within different ELS and SNS environments.

Study Limitations

The first limitation identified in this study was that the study was conducted at a small private university in the Southeast United States. The sample was relatively small, and the response rate of 16% was low, and comprised of non-traditional students. Further research is needed in different geographical regions with traditional student populations. Further research is also needed in different types of institutions, as well as with a variety

of user types (Wozney, Venkatesh, & Abrami, 2006). The second limitation identified in this study was the age of the participants. Of the student participants, 53% were older than 35 years and 71% of the faculty members were older than 40 years of age. As younger age populations have been shown to be less concerned with PISP (WSJ, 2010), this study may not be generalizable to the general population. The third limitation identified in this study was that the invitations to participate in this study were sent by e-mail. This raises the possibility that users who infrequently check their email may have missed the opportunity to participate in the study.

Future Research

Several areas of future research were identified. Future research should be conducted at a larger institution in a different geographical area. Additionally, future research should be conducted at an institution that has more of a traditional student population. Future research should be conducted by performing an experimental study similar to this study after users have attended an awareness program. Additionally, future research could be conducted to develop a predictive model of what specific user actions lead to identity theft. Future research should be conduct in non-educational settings to determine if a difference exists between student and non-student responses. Further research should also be conducted within other types of social networking and e-learning environments. Lastly, as this study confirms prior research results regarding the influence of habit on behavior, further research should be conducted regarding the role of habit within SNS and ELS environments.

Summary

This dissertation investigated the continuing and ever-escalating problem of identity theft (Anderson et al., 2008). Researchers such as Anderson et al., (2008) and Furnell et al., (2008) have suggested that risky online sharing of personal information contributes to the problem of identity theft. Additionally, it has been suggested that users' lack of awareness of the threats to their personal information also contributes to the problem of identity theft (Furnell, 2008). Power and Trope (2006) suggested that users' habits may also have an influence on their practices. Due to the increased use of SNS and ELS, it has been suggested that additional research needs to be conducted regarding users' awareness, habits, and practices while using these environments (Anderson et al., 2008; Chipperfield & Furnell, 2010; Furnell, 2008).

The first factor identified in literature identified as a possible contributor to users' exposure to identity theft was awareness of personal information sharing (Furnell, 2007). Research generally suggests that poor personal information sharing awareness is a key contributor to identity theft (Furnell, 2008). In recent years, personal information has been shared much more frequently and freely, due to the increased popularity of SNS and ELS (Dwyer et al., 2007; Furnell, 2008; Boyd & Ellison, 2007).

The main research question this study addressed was: What is the difference between users' PISA, PISH, and PISP within SNS and ELS? In answering this question, this research developed a new instrument, largely from previously validated research, with which to answer the main research question. To answer this question, this study addressed 12 hypothesis statements:

H1a: There will be no statistically significant effect of SNS users' PISA on their PISP. Failed to reject.

H1b: There will be no statistically significant effect of ELS users' PISA on their PISP. Failed to reject.

H2a: There will be no statistically significant effect of SNS users' PISA on their PISH. Failed to reject.

H2b: There will be no statistically significant effect of ELS users' PISA on their PISH. Failed to reject.

H3a: There will be no statistically significant effect of SNS users' PISH on their PISP. Rejected.

H3b: There will be no statistically significant effect of ELS users' PISH on their PISP. Rejected.

H4a: There will be no statistically significant difference between users' PISA within SNS and users' PISA within ELS, when controlling for gender. Failed to reject.

H4b: There will be no statistically significant difference between users' PISA within SNS and users' PISA within ELS, when controlling for age. Failed to reject.

H5a: There will be no statistically significant difference between users' PISH within SNS and users' PISH within ELS, when controlling for gender. Partially rejected.

H5b: There will be no statistically significant difference between users' PISH within SNS and users' PISH within ELS, when controlling for age. Partially rejected.

H6a: There will be no statistically significant difference between users' PISP within SNS and users' PISP within ELS, when controlling for gender. Failed to reject.

H6b: There will be no statistically significant difference between users' PISP within SNS and users' PISP within ELS, when controlling for age. Rejected.

To address the hypothesis statements, a three-section survey instrument was developed using items from Verplanken et al. (2005), Limayem et al. (2007), Shaw et al. (2009), de Bruijn and van den Putte (2009), as well as Furnell (2008). The PISH section of the instrument used items from the SRHI, therefore, the internal validity was already established. The PISP section of the instrument used items from Fogel and Nehmad (2009), which had also already established internal validity. The PISA section of the survey instrument used sections of surveys previously conducted by Shaw et al. (2009) and as Furnell (2008). Therefore, this section of the survey was validated for internal reliability.

The first section of the survey instrument addressed PISH, and consisted of items from the SRHI (Verplanken et al., 2005), and contained 12 items on a five-point Likert scale. The second section of the survey instrument addressed PISP, and consisted of 12 items on a yes/no scale (Fogel & Nehmad, 2009). The third section of the survey instrument addressed PISA, and consisted of four items on a five-point Likert scale (Shaw et al., 2009; Furnell, 2008). Each of the three sections asked about both SNS and ELS. The fourth section of the survey addressed asked the participants if they had been or knew of someone who had been a victim of identity theft. The final section, the demographics section, was comprised of eight variables (gender, age, marital status, highest level of education completed, years using a computer, years using the Internet, current computer usage, number of previous e-learning courses taken).

A total of 296 students and 94 faculty members completed the Web-based survey. Pre-analysis data screening was conducted to identify cases of response set bias and outliers. Two cases were identified as outliers and were eliminated from further analysis. Results from the Cronbach's Alpha identified two of the constructs as problematic and that the Cronbach's Alpha would be higher if the items were deleted. PISH4S and PISH10S were deleted from the data set. Cronbach's Alpha was re-run and resulted in the following scores: PISH_S was .947; PISH_E was .913; PISA_S was .877; and PISA_E was .89.

In the preceding section, three limitations were identified, followed by a discussion on the implications of this research for future use in the field of IS. Additionally, recommendations were made to further this research and build on the body of knowledge. Finally, a summary of this study's findings was provided.

This study compared PISA, PISH, and PISP within SNS and ELS environments. Information security awareness has been studied at length and has a significant foundation of data. This study improves upon the previous studies of awareness and suggests that there are additional factors to consider to consider in attempting improve users' PISP. As reported in this study, PISP was not significantly influenced by awareness. However, PISH significantly influenced PISP, suggesting that additional studies need to be conducted and opening fascinating and exciting areas or research.

1

2

3

4

Appendix A

Survey Instrument

Please respond to the following statements from one to five, where one (1) indicates "Not at all" and five (5) indicates "Extremely" regarding your perception about sharing personal information posted to Facebook©

Item	Not at all (1)	Slightly (2)	Moderately (3)	Very (4)	Extremely (5)
PISA_SN1: To what extent do you think that Facebook© shares your personal information with other companies?	Not at all (1)	Slightly (2)	Moderately (3)	Very (4)	Extremely (5)
PISA_SN2: To what extent do you think about your personal information being shared by Facebook©?	Not at all (1)	Slightly (2)	Moderately (3)	Very (4)	Extremely (5)
PISA_SN3: To what extent do you think that other individuals use any information you provided on Facebook©?	Not at all (1)	Slightly (2)	Moderately (3)	Very (4)	Extremely (5)
PISA_SN4: To what extent do you think about your personal information provided on Facebook© being shared by employees of Facebook©?	Not at all (1)	Slightly (2)	Moderately (3)	Very (4)	Extremely (5)

Please respond to the following statements from one to five, where one (1) indicates "Not at all" and five (5) indicates "Extremely" regarding your perception about sharing personal information posted to Blackboard©:

Item	Not at all (1)	Slightly (2)	Moderately (3)	Very (4)	Extremely (5)
PISA_EL1: To what extent do you think your university shares your personal information posted on Blackboard© with other companies?	Not at all (1)	Slightly (2)	Moderately (3)	Very (4)	Extremely (5)
PISA_EL2: To what extent do you think about your personal information posted on Blackboard© is being shared by your university?	Not at all (1)	Slightly (2)	Moderately (3)	Very (4)	Extremely (5)
PISA_EL3: To what extent do you think that other individuals use any information you provided on Blackboard©?	Not at all (1)	Slightly (2)	Moderately (3)	Very (4)	Extremely (5)
PISA8: To what extent do you think about your personal information provided on Blackboard© being shared by employees at the university?	Not at all (1)	Slightly (2)	Moderately (3)	Very (4)	Extremely (5)

Please respond to the following statements from one to five, where one (1) indicates "Strongly disagree" and five (5) indicates "Strongly agree" for each of the given statements regarding the personal information you share on Facebook© and Blackboard©

Item	Facebook©					Blackboard©				
	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)
PISH1: Sharing personal information via … is something I do frequently.	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)
PISH2: Sharing personal information via … is something I do automatically.	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)
PISH3: Sharing personal information via … is something I do without having to consciously remember.	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)
PISH4: Sharing personal information via … is something that makes me feel weird if I do not do it.	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)
PISH5: Sharing personal information via … is something I do without thinking.	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)
PISH6: Sharing personal information via … is something that would require effort not to do it.	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)
PISH7: Sharing personal information via … is something that belongs to my (daily, weekly, monthly) routine.	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)

Item	Facebook©					Blackboard©				
	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)
PISH8: Sharing personal information via … is something I start doing before I realize I'm doing it.	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)
PISH9: Sharing personal information via … is something I would find hard not to do.	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)
PISH10: Sharing personal information via … is something I have no need to think about doing.	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)
PISH11: Sharing personal information via … is something that's typically "me."	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)
PISH12: Sharing personal information via … is something I have been doing for a long time.	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)	Strongly Disagree (1)	Disagree (2)	Neither Agree nor Disagree (3)	Agree (4)	Strongly Agree (5)

Please respond to the following statements with a Yes or No, regarding the personal information you share on Facebook© and Blackboard©.

Item	Facebook©	Blackboard©
PISP1: Do you have your own profile online that others can see?	Yes/No	Yes/No
PISP2: Do you allow anyone to see your profile?	Yes/No	Yes/No
PISP3: Do you include a picture of yourself on your profile?	Yes/No	Yes/No
PISP4: Do you include your email address on your profile?	Yes/No	Yes/No
PISP5: Do you include your instant messenger address on your profile?	Yes/No	Yes/No
PISP6: Do you include your phone number on your profile?	Yes/No	Yes/No
PISP7: Do you include your home address on your profile?	Yes/No	Yes/No
PISP8: Do you include information about your interests and/or hobbies on your profile?	Yes/No	Yes/No
PISP9: Do you include information about your personality on your profile?	Yes/No	Yes/No
PISP10: Do you write or comment about other people's profile pages?	Yes/No	Yes/No
PISP11: Do you spend time personalizing your profile page?	Yes/No	Yes/No
PISP12: Do you use your real name on your profile page?	Yes/No	Yes/No

Have you or someone you know been a victim of identity theft or other unauthorized use of your personal information?

IDT1. You have personally been a victim of identity theft or other unauthorized use of your personal information	Y/N
IDT2. Someone in your family has been a victim of identity theft or other unauthorized use of their personal information	Y/N
IDT3. Someone in your workplace or school has been a victim of identity theft or other unauthorized use of their personal information	Y/N

Please provide the following demographic information.

Gender:	□ Male	□ Female			
Age:	□ 18 or under	□ 19-24	□ 25-29	□ 30-34	□ 35-39
	□ 40-44	□ 45-54	□ 55-59	□ 60 or older	
Marital status	□ Married	□ Single	□ Divorced	□ Separated	□ Widowed
Highest level education completed	□ Graduated from high school or GED	□ Vocatio-nal or trade school	□ Bachelor degree	□ Post-graduate Diploma	□ Master Degree
Years using computers	[_____]				
Years using the Internet	[_____]				
Current Computer usage		□ Daily, more than 5 hours		□ Daily, less than 5 hours	
		□ Not every day, but more than once a week		□ Less than once a week	
Number of previous e-learning courses taken		□ 0	□ 1	□ 2	□ 3
		□ 4	□ 5-9	□ 10 or more	

Appendix B

Expert Review Questionnaire

Thanks for participating in this review. Please provide your feedback regarding the research instrument attached. If required, please use additional paper.

1. Are the directions for completing the instrument clear and complete?	**YES**	**NO**
If no please explain		
2. Do the items appropriately measure the construct being evaluated?	YES	NO
If no please explain		
3. Are there items that you would recommend revising?	YES	NO
If yes please explain		

4. Would you recommend deleting any items? YES NO

If yes please explain

5. Would you recommend including any additional items in this proposed instrument? YES NO

If yes please explain

GENERAL COMMENTS

1

Appendix C

E-Mail to Expert Panel

Hello,

My name is Albert Ball and I am a Ph.D. student at the Graduate School of Computer and Information Sciences, Nova Southeastern University. Currently, I am working on my dissertation research titled “A Comparison of Users’ Personal Information Sharing Awareness, Habits, and Practices in Social Networking Sites and E-Learning Systems”. This study will attempt to assess the influence of users’ personal information sharing awareness (PISA) on their personal information sharing habits (PISH) and personal information sharing practices (PISP), as well as to compare the three constructs between SNS and ELS. This information obtained from this study could prove valuable in understanding users PISP, based on their PISA and PISH within ELS and SNS.

I am inviting you to participate in this study as a member of an expert panel, by completing an anonymous online survey. Participation in this survey is at your discretion and I will not know who completes this survey.

Attached to this e-mail is a copy of the preliminary survey instrument. Your assistance is being sought, as an expert, to review the preliminary instrument and perform a qualitative evaluation of the instruments validity by answering five questions. Your responses to

these questions will assist in making a determination of whether or not the individual items serve to measure the constructs being evaluated and in the identification of additional items that could enhance the instrument. Additionally, there will be a general comments section where you can provide information on the content and structure of the instrument. Your feedback will be used to adjust the attached instrument as required. The survey should take approximately 30 to 45 minutes to complete, however, you may take as much time as you choose. Once completed, please click the "Done" button to submit the completed survey. Any information provided will only be used as part of this study.

If you are willing to participate, please click on the link below for access.

(the survey URL link was inserted here upon the creation of the survey)

Your completion of the survey indicates your voluntary participation. If you have any questions regarding this study, you may contact me at aball@hodges.edu.

Thanks for your consideration and I appreciate your assistance.

Regards

Albert L. Ball

Appendix D

Follow-up E-Mail to Expert Panel

My name is Albert Ball and I am a Ph.D. student at the Graduate School of Computer and Information Sciences, Nova Southeastern University. Currently, I am working on my dissertation research titled "A Comparison of Users' Personal Information Sharing Awareness, Habits, and Practices in Social Networking Sites and E-Learning Systems". Your assistance is being sought, as an expert, to review the preliminary instrument and perform a qualitative evaluation of the instruments validity by answering five questions. Your responses to these questions will assist in making a determination of whether or not the individual items serve to measure the constructs being evaluated and in the identification of additional items that could enhance the instrument. Additionally, there will be a general comments section where you can provide information on the content and structure of the instrument. Your feedback will be used to adjust the attached instrument as required. The survey should take approximately 30 to 45 minutes to complete, however, you may take as much time as you choose. Once completed, please click the "Done" button to submit the completed survey. Any information provided will only be used as part of this study.

If you are willing to participate, please click on the link below for access.
(the survey URL link was inserted here upon the creation of the survey)

Your completion of the survey indicates your voluntary participation. If you have any questions regarding this study, you may contact me at aball@hodges.edu.

Thanks for your consideration and I appreciate your assistance.

Regards

Albert L. Ball

Appendix E

E-Mail to Main Population

Hello,

My name is Albert Ball and I am a Ph.D. student at the Graduate School of Computer and Information Sciences, Nova Southeastern University. Currently, I am working on my dissertation research titled “A Comparison of Users’ Personal Information Sharing Awareness, Habits, and Practices in Social Networking Sites and E-Learning Systems”.

I am inviting you to participate in this study by completing an anonymous online survey. Participation in this survey is at your discretion and I will not know who completes this survey.

The survey will comprise 32 questions. The questions should take no more than 20 minutes to complete however you may take as much time as you choose. Once completed, please click the “Done” button to submit the completed survey. Any information provided will only be used as part of my research.

If you are willing to participate, please click on the link below for access.
(the survey URL link was inserted here upon the creation of the survey)

Your completion of the survey indicates your voluntary participation. If you have any questions regarding this study, you may contact me at aball@hodges.edu.

Thanks for your consideration and I appreciate your assistance.

Regards

Albert L. Ball

Appendix F

Follow-up E-Mail to Main Population

My name is Albert Ball and I am a Ph.D. student at the Graduate School of Computer and Information Sciences, Nova Southeastern University. Currently, I am working on my dissertation research titled "A Comparison of Users' Personal Information Sharing Awareness, Habits, and Practices in Social Networking Sites and E-Learning Systems".

If you are willing to participate, please click on the link below for access.

(the survey URL link was inserted here upon the creation of the survey)

Participation in this survey is at your discretion and I will not know who completes this survey. Your completion of the survey indicates your voluntary participation. If you have any questions regarding this study, you may contact me at aball@hodges.edu.

Thanks for your consideration and I appreciate your assistance.

Regards

Albert L. Ball

Appendix G

IRB Approval Letter

NOVA SOUTHEASTERN UNIVERSITY
Office of Grants and Contracts
Institutional Review Board

MEMORANDUM

To: Albert Ball

From: Ling Wang, Ph.D.
Institutional Review Board

Date: April 18, 2012

Re: *A Comparison of Users' Personal Information Sharing Awareness, Habits, and Practices in Social Networking Sites and E-Learning Systems*

IRB Approval Number: wang04151203

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) CONSENT: If recruitment procedures include consent forms these must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2) ADVERSE REACTIONS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and 954-262-2020 respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Protocol File

3301 College Avenue • Fort Lauderdale, FL 33314-7796 • (954) 262-5369
Fax: (954) 262-3977 • Email: *ingw@nsu.nova.edu* • Web site: www.nova.edu/cwis/ogc

Appendix H

Approval Letter to Collect Data from Hodges University

HODGES UNIVERSITY

December 13, 2011

To whom it may concern:

Please be advised that Albert Ball has the permission of Hodges University to collect data from the students and faculty related to their personal information sharing practices in furtherance of his doctoral studies at Nova Southeastern University.

If you have any questions, please let me know.

Sincerely,

Jeanette Brock

Jeanette Brock, J.D.
Executive Vice President of Academic Affairs

References

Acquisti, A. & Gross, R. (2006). Imagined communities: Awareness, information sharing and privacy on the Facebook©. *Privacy Enhancing Technologies, 4528/2006*, 36-58.

Ajzen, I. (2002). Residual effects of past on later behavior: Habituation and reasoned action perspectives. *Personality and Social Psychology Review, 6*(2), 107-122.

Anderson, K. B., Durbin, E., & Salinger, M. A. (2008). Identity theft. *Journal of Economic Perspectives, 22*(2), 171-192.

Anwar, M., Greer, J., & Brooks, C. (2006). Privacy enhanced personalization in e-learning. *Proceedings of the 2006 International Conference on Privacy, Security and Trust, 380*(1), 42.

Ball, D. M., & Levy, Y. (2008). Emerging educational technology: Assessing the factors that influence instructors' acceptance in information systems and other classrooms. *Journal of Information Systems Education, 19*(4), 431-444.

Bargh, J. A. (1994). The four horsemen of automaticity: Awareness, intention, efficiency, and control in social cognition. In: R.S. Wyer & T.K. Srull (Eds.), *Handbook of Social Cognition* (vol.1, pp.1-40). Hillsdale, NJ: Erlbaum.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9). Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/1394

Bellah, J. (2001). Training: Identity theft. *Law & Order, 49*(10), 222-227.

Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in e-commerce: Stated preferences vs. actual behavior. *Communications of the ACM, 48*(4), 101-106.

Blackboard© (2010). Blackboard. http://www.blackboard.com.

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

Burton-Jones, A., & Hubona, G. S. (2006). The mediation of external variables in the technology acceptance model. *Information & Management, 43*, 706-717.

Cazier, J. A., Wilson, E. V., & Medlin, B. D. (2007). The role of privacy risk in IT acceptance: An empirical study. *International Journal of Information Security and Privacy, 1*(2), 61-73.

Chipperfield, C., & Furnell, S. (2010). From security policy to practice: Sending the right messages. *Computer Fraud & Security, 10*(3), 13-19.

Clark, F., Sanders, K., Carlson, M., Blanche, E., & Jackson, J. (2007). Synthesis of habit theory. *OTJR: Occupation, Participation and Health*, *27*(4), 7S-23S.

Cooper, D. R., & Schindler, P. S. (2006). *Business research methods* (9th ed.). New York: McGraw-Hill.

Dalsgaard, C. (2006). Social software: E-learning beyond learning management systems. *European Journal of Open, Distance and E-learning, 2006*(II). Retrieved from http://www.eurodl.org/materials/contrib/2006/Christian_Dalsgaard.htm

de Bruijn, G. J. & van den Putte, B. (2009). Adolescent soft drink consumption, television viewing and habit strength. Investigating clustering effects in the theory of planned behavior. *Appetite, 53*(1), 66-75.

de Bruijn, G. J., & Kremers, S. P. J., De Vet, E., de Nooijer, J., van Mechelen, W., & Brug, J.(2007). Does habit strength moderate the intention-behavior relationship in the Theory of Planned Behavior? The case of fruit consumption, *Psychology & Health, 22*(8), 899-916.

de Bruijn, G. J., Kremers, S. P. J., Singh, A., van den Putte, B., & van Mechelen, W. (2009). Adult active transportation adding habit strength to the theory of planned behavior. *American Journal of Preventive Medicine*, *36*(3), 189-194.

de Bruijn, G. J., Kroeze, W., Oenema, A., & Brug, B. (2008). Saturated fat consumption and the theory of planned behavior: Exploring addictive and interactive efforts of habit strength. *Appetite 51*(2), 318-323.

Diaz, J., Arroyo, D., & Rodriguez, F. B. (2011). An approach for adapting Moodle into a secure infrastructure. *Computational Intelligence In Security for Information Systems, 6694*(2011), 6-27.

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

Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and privacy concerns within social networking sites: A comparison of facebook and myspace. *Proceedings of the thirteenth Americas Conference on Information Systems.* Keystone, CO., 339-351.

El-Khatib, K., Korba, L., Xu, Y., & Yee, G. (2003). Privacy and security in e-learning. *International Journal of Distance Education, 1*(4), 1-19.

eListen® Software (2006). eListen. [Computer software]. http://www.eListen.com.

Ellison, N. B., Steinfield, C., & Lampe, C. (2011). Connection strategies: Social capital implications of Facebook-enabled communication practices. *New Media & Society, 13*(6), 873-892.

Ferdousi, B., & Levy, Y. (2010). Development and validation of a model to investigate the impact of individual factors on instructors' intention to use e-learning systems. *Interdisciplinary Journal of E-learning and Learning Objects, 6,* 1-21.

Fogel, J., & Nehmad, E. (2009). Internet social networking communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25*(1), 153-160.

Furnell, S. (2008). End-user security culture a lesson that will never be learnt? *Computer Fraud & Security, 2008*(4), 6-9.

Furnell, S. (2010). Jumping security hurdles. *Computer Fraud & Security, 2010*(6), 10-14.

Furnell, S., Bryant, P., & Phippen, A. (2007). Assessing the security perceptions of personal internet users. *Computers & Security, 26*(1), 410-417.

Furnell, S., Tsaganidi, V., & Phippen, A. (2008). Security beliefs and barriers for novice internet users. *Computers & Security, 27*(7-8), 235-240.

Gaw, S. (2009). Ideas and Reality: Adopting secure technologies and developing secure habits to prevent message disclosure. *Dissertation Proquest* (UMI. No. 3356710).

Gefen, D. (2003). TAM or just plain habit: A look at experience online shoppers. *Journal of End User Computing, 15*(3), 1-13.

Gefen, D., Straub, D. W., & Boudreau, M. C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems, 4*(7), 1-77.

Generation Y highly susceptible to threats due to risky behavior online, (2010, April 20). The *Wall Street Journal* (U. S. Edition). Retrieved from http://online.wsj.com.

Gerking, K. L., Taylor, T. H., & Weatherby, F. M. (2009). The perception of learning and satisfaction of nurses in the online environment. *Journal for Nurses in Staff Development, 25*(1), E8-E13.

Gross, R. & Acquisti, A. (2005). Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, New York, 71-80.

Hair, J. F., Anderson, R. E., Tatham, R. L., & Black. W. C. (1984). *Multivariate data analysis.* Upper Saddle River, New Jersey: Prentice Hall.

Hart, D. (2008). Attitudes and practices of students towards password security. *Journal of Computing Sciences in Colleges, 23*(5), 169-174.

Hazari, S., Haragrave, W., & Clenney, B. (2008). An empirical investigation of factors influencing information security behavior. *Journal if Information Privacy & Security, 4*(4), 3-20.

Hogarth, K. & Dawson, D. (2008). Implementing e-learning in organizations: What e-learning research can learn from instructional technology (IT) and organizational studies (OS) innovation studies. *International Journal on E-learning, 7*(1), 87-105.

Kremers, S. P. J., Brug, J. (2008). Habit strength of physical activity and sedentary behavior among children and adolescents. *Pediatric Exercise Science, 20*(1), 5-17.

Kritzinger, E. (2006). Information security in an e-learning environment. Education in the 21ST Centurey - *Impact of ICT and Digital Resources IFIP International Federation for Information Processing. 210*(2006), 345-349.

Kritzinger, E., & von Solms, S. H. (2006). E-learning: Incorporating information security governance. *Issues in Informing Science and Information Technology, 3,* 319-325.

Kumar, N., Mohan, K., & Holowczak, R. (2008). Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems, 46*(1), 254-264.

Lai, F., Li, D., & Hsieh, C. T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems, 52*(2), 353-363.

Lankton, M. K., Wilson, E. V., & Mao, E. (2010). Antecedents and determinants of information technology habit. *Information & Management, 47*(6), 300-307.

Lawler, J. P. & Molluzo, J. C. (2011). A survey of first-year college student perceptions of privacy in social networking. *Journal of Computing Sciences in Colleges, 26*(3), 36-41.

Levy, Y. (2006). *Assessing the value of E-learning systems.* Hershey, PA: Information Science Publishers.

Levy, Y. (2007). Comparing dropouts and persistence in e-learning courses. *Computers & Education, 48*(2), 184-204.

Levy, Y. (2008). An empirical development of critical value factors (CVF) of online learning activities: An application of activity theory and cognitive value theory. *Computers & Education, 51*(4), 1664-1675.

Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science, 9*, 181-212.

Levy, Y., & Murphy, K. E. (2002). Toward a value framework for online learning systems. *Proceeding of the 35th Hawaii International Conference on System Sciences*, Big Island, Hawaii, 5-14.

Levy, Y., & Ramim, M. M. (2009). Initial development of a learners' ratified acceptance of multibiometrics intentions model (RAMIM). *Interdisciplinary Journal of E-Learning and objects, 5*, 378-319.

Li, R. Y. M., & Poon, S. W. (2011). Using Web 2.0 to share knowledge of construction safety: The fable of economic animals. *Economic Affairs, 31*(1), 73-79.

Limayem, M. & Hirt, S. G. (2003). Force of habit and information systems usage: Theory and initial validation. *Journal of the Association for information Systems, 4*(1), 65-97.

Limayem, M., & Cheung, C. M. K., (2008). Understanding information systems continuance: The case of internet-based learning technologies. *Information & Management, 45*(4), 227-232.

Limayem, M., Hirt, S. G., & Cheung, C. M. K., (2007). How habit limits the predictive power of intention: The case of information systems continuance. *MIS Quarterly, 31*(4), 705-737.

Mazer, J. P., Murphy, R. E., & Simonds, C. J. (2007). I'll see you on "Facebook": The effects of computer-mediated teacher self-disclosure on student motivation, affective learning, and classroom climate. *Communication Education, 56*(1), 1-77.

McAfee/NCSA. Cyber security survey newsworthy analysis, (October, 2007). *McAfee, National Cyber Security Alliance.* Retrieved from http://mcafee.com/.

McDaniel, G. (1994). *IBM dictionary of computing.* New York: McGraw-Hill.

Mertler, C., & Vanatta, R. (2010). *Advanced and multivariate statistical methods: Practical application and interpretation* (4th ed.). Los Angeles: Pyrczak.

Norberg, P. A., Horne, D. R., & Horne, D. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs, 41*(1), 100-126.

Nosek, B. A., Hawkins, C. B., & Frazier, R. S. (2011). Implicit social cognition: from measures to mechanisms. *Trends in Cognitive Science, 15*(4), 152-159.

Nunnally, J. C. (1967). *Psychometric theory.* New York: McGraw-Hill

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory.* New York: McGraw-Hill.

Ong, C., Lai, J., & Wang, Y. (2004). Factors affecting engineers' acceptance of asynchronous e-learning systems in high-tech companies. *Information & Management, 41*(6), 795-804.

Oceja, L., Ambrona, T., Lopez-Perez, B., Salgado, S., & Villegas, M. (2010). When the victim is on among others: Empathy, awareness of others and motivational ambivalence. *Motivation and Emotion, 34*(2), 110-119.

Ortiz de Guinea, A., Markus, M. L. (2009). Why break the habit of a lifetime? Rethinking the role of intention, habit, and emotion in continuing information technology use. *MIS Quarterly, 33*(3), 433-444.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*(1), 27-41.

Power, E. M., & Trope, R. L. (2006). The 2006 survey of legal developments in data management, privacy, and information security: The continuing evolution of data governance. *The Business Lawyer, 62*(1), 251-295.

Ramim, M., & Levy, Y. (2006). Securing e-learning systems: A case of insider cyber attacks and novice IT management in a small university. *Journal of Cases on Information Technology, 8*(4), 24-34.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security, 27*(7-8), 241-253.

Roblyer, M. D., McDaniel, M., Webb, M. Herman, J. & Witty, J. V. (2010). Findings on Facebook in higher education: A comparison of college faculty and student uses and perceptions of social networking sites. *Internet and Higher Education, 13,* 134-140.

Roscoe, J. T. (1975). Fundamental research statistics for the behavioral sciences, New York: Holt.

Ruiz, J. G., Mintzer, M., & Leipzig, R. M. (2006). The impact of e-learning in medical education. *Academic medicine, 81*(3), 207-212.

Sekaran, U. (2003). *Research methods for business - A skill building approach*. Hoboken, NJ: John Wiley & Sons.

Selim, H. M. (2007). Critical success factors for e-learning acceptance: Confirmatory factor models. *Computers & Education, 49*(2), 396-413.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education, 52*(1), 92-100.

Shaw, R. S., Keh, H. C., & Haung, N. C. (2011). Information security awareness on-line materials design with knowledge maps. *International Journal of Distance Education Technologies, 9*(1), 41-56.

Short, J. (2008). Risk in a Web 2.0 world. *Risk Management, 55*(10), 28-32.

Skeels, M. M., & Grudin, J. (2009). When Social Networks Cross Boundaries: A Case Study of Workplace Use of Facebook and LinkedIn. *Proceedings of the ACM 2009 International Conference on Supporting Group Work.* Sanibel, FL., 95-104.

SPSS® Software (2006). SPSS. [Computer software]. http://www.spss.com.

Strater, K. & Lipford, H. R. (2008). Strategies and struggles with privacy in an online social networking community. *BCS-HCI '08 Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction* 1, 111-119.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly, 13*(2), 147-169.

Straub, D. W., Rai, A. & Klein, R. (2004). Measuring firm performance at the network level: A nomology of the business impact of digital supply networks. *Journal of Management Information Systems, 21*(1), 83-114.

Sturgeon, C. M. & Walker, C. (2009). Faculty on facebook: Confirm or deny? *14th Annual Instructional Technology Conference Middle Tennessee State University,* Murfreesboro, TN. Retrieved July 16, 2010 from http://www.cmsturgeon.com/itconf/facebook-report.pdf

Tabachnick, B. G. & Fidell, L. S. (2007). Using Multivariate statistics (5th ed). Boston, MA: Allyn & Bacon.

Teltzrow, M., & Kobsa, A. (2004). Impacts of user privacy preferences on personalized systems: A comparative study. In Karat, C.M., Blom, J., Karat, J., eds., Designing Personalized User Experiences in eCommerce. Kluwer Academic Publishers, Dordrecht, Netherlands, 2004, 315–332.

Thompson, L. A., Dawson, K., Ferdig, R., Black, E. W., Boyer, J., Cotts, J. & Black, N. P. (2008). The intersection of online social networking with medical professionalism. *Journal of General Internal Medicine, 23*(7), 954-957.

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating information security awareness: Research and practice gaps. *Information Security Journal: A Global Perspective, 17*(5), 207-227.

Udo, G. (2001). Privacy and security concerns as major barriers for e-commerce: A survey study. *Information Management & Computer Security, 9*(4), 165-174.

Van Niekerk, J. F. & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security, 29*(1), 476-486.

van Raaij, E. M., & Schepers, J. J. L. (2008). The acceptance and use of a virtual learning environment in China. *Computers & Education, 50*(3), 838-852.

Verplanken, B., & Aarts, H. (2006). Beyond frequency: Habit as mental construct. *British Journal of Social Psychology, 45*(3), 639-656.

Verplanke, B., & Melkevik, O. (2008). Predicting habit: The case of physical exercise. *Psychology of Sports and Exercise, 9*(1), 15-26.

Verplanken, B., & Orbell, S. (2003). Reflections of past behavior: A self-report index of habit strength. *Journal of Applied Social Psychology, 33*(6), 1313-1330.

Verplanken, B., Myrbakk, V., & Rudi, E. (2005). The measurement of habit. In Betsch, T., & Haberstroh, S: The Routines of Decision Making. Laurence Erlbaum: Mahwah, NJ, 2005, 231-247.

Webber, C. G., Lima, M. W. P., Casa, M. E., & Ribeiro, A. M. (2007). Towards secure e-learning applications: A multiagent platform. *Journal of Software, 2*(1), 60-69.

Weippl, E. R. (2005). *Security in elearning.* New York, NY: Springer-Verlag.

Winkler, J. K., Kanouse, D. E., & Ware, J. E. (1982). Controlling for acquiescence response set in scale development. *Journal of Applies Psychology, 67*(5), 555-561.

Wozney, L., Venkatesh, V., & Abrami, P. (2006). Implementing computer technologies: Teachers' perceptions and practices. *Journal of Technology and Teacher Education, 14*(1), 173-207.

Wu, Y. C., Andoh-Baidoo, F. K., Crossler, R., & Tanquma, J. (2011). An exploratory study of the security management practices of Hispanic students. *International Journal of Security, 5*(1), 1-61.

Yeh, K. (2009). *Reconceptualizing technology use and information system success: Developing and testing a theoretically integrated model.* Information Systems & Operations Management). *ProQuest Dissertations and Theses,* Retrieved from http://ezproxylocal.library.nova.edu/login?url=http://search.proquest.com/docview/305180497?accountid=6579

Zhang, D., Zhao, J. L., Zhou, L., & Nunamaker, J. F. (2004). Can e-learning replace classroom learning? *Communications of the ACM, 47*(5), 75-81.

Zukowski, T., & Brown, I. (2007). Examining the influence of demographic factors on Internet users' information privacy concerns. *SAICSIT'07, Conference of the South African Institute of Computer Scientists and Information Technologists.* Port Elizabeth, ZA: 226, 197-204.