*Online Journal of Applied Knowledge Management*
A Publication of the International Institute for Applied Knowledge Management

*Volume 3, Issue 1, 2015*

# Examining users' personal information sharing awareness, habits, and practices in social networking sites and e-learning systems

**Albert L. Ball,** *Hodges University, Fisher School of Technology, aball@hodges.edu*

**Michelle M. Ramim,** *Hodges University, Fisher School of Technology, mramim@hodges.edu*

**Yair Levy,** *Nova Southeastern University, Graduate School of Computer and Information Sciences, levyy@nova.edu*

## Abstract

*Reports of identity theft continue to be widely reported, while users continue to share 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. However, even among users who claim to be aware of security threats, actual awareness is still lacking. Research indicates that users' habits influence their practices. However, the relationship between habit and practices is not always clear. Habit theory has been validated across many disciplines, with very limited attention in Information Systems. Thus, the main goal of this study was to assess the influence of users' personal information sharing awareness (PISA) on their habits (PISH) and practices (PISP), while comparing the three constructs between SNS and ELS. Empirical survey instrument was developed based on prior literature. A total of 390 responses were received, and path analysis was conducted to test the hypotheses. All three constructs demonstrated high reliability. Users' habits were determined to have the strongest influence on their practices. Information gained from this study may help organizations in the development of better approaches to the securing users' personal information.*

***Keywords**: Information sharing awareness, E-learning systems, habits, practices, Social Networking Sites.*

## Introduction

*"But he that filches from me my good name/Robs me of that
which not enriches him/And makes me poor indeed" (Shakespeare, Othello)*

Identity theft continues to be a modern day crisis that eventually affects every person who uses the Internet (Anderson, Durbin, & Salinger, 2008; Lai, Li, & Hsieh, 2012). Identity theft is "the unlawful use of another's personal identifying information" (Bellah, 2001, p. 222). Contributing to this problem is users' risky online sharing of personal information, which has been found to increase the risk of misuse of their personal information (Anderson et al., 2008; Furnell, Tsaganidi, & Phippen, 2008). However, many people find securing their personal information and systems to be cumbersome as well as frustrating. Others may feel that information security obstructs their access to information or online resources (Chipperfield & Furnell, 2010).

Information security in a personal context 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). 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 aware of the risks, or are 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 in literature that additional research is needed to better understand users’ practices regarding their personal information sharing while using SNS and ELS (Anderson et al., 2008; Chipperfield & Furnell, 2010; Furnell, 2008; 2010).

According to Hovav and Gray (2014), information security threats are increasing, putting users’ personal information at risk on a daily basis. These threats are compounded by the unwillingness or inability of many users to protect themselves from security attacks (Furnell et al., 2008). On one hand, the increase in threats can be attributed to risky user online practices related to the sharing of personal information (Furnell, 2008; Wall Street Journal, 2010). On the other hand, it was found that many IS users are willing to accept increased risk in return for convenience (Furnell et al., 2008; Vance, Lowry, & Eggett, 2013). For example, due to the varied security requirements associated with different IS, many users store usernames and passwords in their systems for convenience. However, users may 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. Moreover, users have been found to regularly participate in risky online personal information sharing while using SNS such as Facebook and Tweeter (Furnell, 2008; Short, 2008). Furthermore, Power and Trope (2006) suggested that users’ habits may also have an influence on their practices. Because of these issues and the risk to users, further investigation into users’ security awareness, information sharing, and their habits has merit (Furnell et al., 2007). Consequently, our main goal in this research study was to assess the influence of users’ personal information sharing awareness (PISA) and personal information sharing habits (PISH) on personal information sharing practices (PISP), while assessing if there are any differences among the three aforementioned constructs within SNS and ELS.

## Theoretical Background

### Personal Information Sharing Awareness (PISA)

Personal information sharing awareness (PISA) refers to the individuals’ awareness of the risks related to their voluntary acts to share their personal information with others. PISA is a sub-category of the more generalized personal information security awareness, which also includes of the individuals awareness of voluntary, non-voluntary, or even information that is taken without their willingness to share (i.e. PII stolen via data breach). While the focus of this paper is on PISA, it is still important to understand the overarching issue of information security awareness (Burley, Eisenberg, & Goodman, 2015). Accordingly, personal information security awareness in general is regarded in the literature as users’ general awareness of security issues and threats to their personal information, as well as users’ responsibilities to act upon that awareness (Furnell, 2008; Rezgui & Marks, 2008). 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). Users represent individuals who are aware and have acted to protect personal information (D'Arcy, Hovav, & Galletta, 2009). Following these definitions in defining PISA as the degree of users’ understanding about the information security threats posed by the sharing of their personal information, combined with the awareness of their responsibilities and acts to exercise sufficient levels of information security control in protecting their personal information.

Though public awareness of identity theft threat has increased substantially, new avenues to identity fraud have contributed to an increasing number of security incidents, including the breach of information privacy, identity theft, fraud, social engineering and cybersecurity threat vectors posed by the unauthorized access and use of personal information (Hovav & Grey, 2014; Zukowski & Brown, 2007). Users may be generally aware of information security threats to their personal information, still they often engage in risky online practices that may increase the risk of exposing their personal information (Anderson et al., 2008; Furnell et al., 2008). It appears that some users may feel overconfident in information security protections such as anti-virus and anti-spyware software leading them to engage in such behavior. With companies increasing their spending on advanced cybersecurity technologies, users perceive that their confidential information is well protected (Asanka, Arachchilage, & Love, 2013).

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 a challenge, as many users are unaware of the proper configuration required for software such as Internet security suites, firewalls, and other technologies used to protect their personal information (Furnell, 2008; Kumar, Mohan, & Holowczak, 2008). Other users are simply unwilling or unable to configure the security devices (Furnell, 2008; Kumar et al., 2008), leading to disastrous consequences. A number of incidents reported in the popular media indicated the cause of breach was the use of the default setting in the hardware (i.e. Bank of Montreal ATMs hack, US emergency alert system hack, US highway notification signs hack, etc.) (Krigsman, 2009). Consequently, IS security cannot be mitigated 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. IS security practitioners agree that educating users about sharing of personal information is needed in order to achieve effective information security, while IS security researchers advocate for additional research on the role of awareness on actual user practices.

## Personal Information Sharing Practices (PISP)

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). According to Phelps, Nowak, and Ferrell (2000), PISP refers to the users' actual behaviors related to the sharing of individual-specific, personally identifiable information (PII). Such PII are being shared by users across multiple types of Web-based systems including ELS and SNS. Users of ELS face an increased risk to their personal information because they often connect to the ELS from unsecured public networks, or may use public computing (i.e. work computer, mobile phones). This underscores the need for awareness of personal information security within ELS (Furnell et al., 2007).

Users overconfidence appears to have a real effect on their habits. While users may be aware of security concerns and claim to engage in good practices, some researchers claim that users' lack of awareness of the nature of the security risks to their personal information 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 Internet users, Berendt et al. (2005) 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 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 PISP (Hart, 2008). According to Hart (2008) and Furnell, Bryant, and Phippen (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).

Additional evidence for weak users' PISP is provided in recent studies in the context of various online interactions. According to Furnell (2008), poor personal information security practices are also evident within social 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 appear to engage in sharing practices. For example, 87% of Facebook users expose personal information (Strater & Lipford, 2008); 37.5% of medical students in a study revealed their area of residence, suggesting a large number of respondents had poor PISP (Thompson et al., 2008); 87.8% of undergraduate students in another study 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). While, 14.4% of undergraduate student in another study stated that their SNS profile was public, while 10.7% reported not knowing whether their profile was public or private (Lawler & Molluzo, 2011). 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 light of the evidence in these studies for users' risky PISP, additional research regarding users' PISP is warranted (Furnell, 2008). Therefore, this study compared users' PISA, PISH, and PISP between SNS and ELS.

## Personal Information Sharing Habits (PISH)

Habit has also been found to impact the behavior of IS users (Limayem & Cheung, 2008; Polites & Karahanna, 2012), including their PISP (Power & Trope, 2006). Habits are defined as "the extent to which people tend to perform behaviors (use IS) automatically because of learning" (Limayem, Hirt, & Cheung, 2007, p. 709). Habits are said to be a series of automatically organized actions triggered by specific cues, and leading to a specific end (Verplanken & Aarts, 2006). 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, Myrbakk, & Rudi, 2005). Limayem et al. (2007) recommended additional research designed to improve understanding of the influence habit has on users' IS practices. Habit has been studied in connection with 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 beyond 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 et al., 2007; Polites & Karahanna, 2012). For example, in one study habit was shown to impact not only users' intention to use IS, but also the 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). Furthermore, IS habit essentially weakened the users' strength of intention to predict users' continued use of IS over time (Limayem & Cheung, 2008).

Habit has been studied in the context other disciplines. For example, habit has been measured as a behavioral frequency, using measures of past and later behavior. Research consistently found that past behavioral frequency is, indeed, a predictor of future behavior (Verplanken & Orbell, 2003). Though not all repeated behaviors constitute habits, therefore, measures of past behavior may not be inadequate in measuring habits (Ajzen, 2002; Lankton et al., 2010). Moreover, habit involves features of automaticity, including lack of awareness and difficulty to control (Limayem et al., 2007). In 2003, Verplanken and Orbell 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.

Lankton et al. (2010) investigated the relationship between habit and prior IT use in a study of undergraduate students. Results indicated that prior IT use had a significant effect on habit. Additionally, IT habits were shown to developed despite low levels of prior use, thus, validating Verplanken and Orbell (2003) conclusion that habit should not be viewed as a measure of frequency of use. Subsequently, SRHI was validated in four studies for validity and reliability convergent validity, correlation between SRHI and behavioral frequency, as well as SRHI and daily and weekly habits. This study will follow the habit definition suggested by Verplanken et al. (2005) and Limayem et al. (2007). Users' PISH is used in the context of personal information sharing behaviors that are done automatically, and without consciousness or thought. Due to the personal information that users are able to post online, it is important to gain a better understanding of the habits and practices of users who engage in personal information sharing activities, especially in the context both SNS and ELS.

## Personal Information Sharing in Social Networking Sites

SNSs are rapidly gaining the attention of academia, as well as industry seeking to gauge users behavior in SNSs (Boyd & Ellison, 2008; Skeels & Grudin, 2009; Sturgeon & Walker, 2009). SNSs are designed as non-secure systems, thus, many users are unaware of the security issues associated with using SNS's (Acquisti & Gross, 2006). Intrinsically, the majority of users share personal information about themselves with other users via the SNS's, their connections with other individuals, places they have visited, timelines, and other personal experiences. Moreover, most users are unaware of the privacy setting choices, opting to go with the default option. Such a practice leads to poor PISP (Barnes, 2006; Skeels & Grudin, 2009; Sturgeon & Walker, 2009). In 1997, sixdegrees.com was one of the first known SNSs introduced on college campuses. Nowadays, the most common SNSs are Facebook, Twitter, Instagram, and LinkedIn. Regardless of the SNS type users opt to use, similar security concerns appear to run across all (Weippl, 2005). One significant concern relates to the removal of boundaries between professional and personal lives as a result of posting personal information in SNS (Skeels & Grudin, 2009).

Many SNSs provide methods for users to post sensitive personal information (Weippl, 2005). For example, users share their birth date, workplace information, addresses, phone numbers, place of birth, childhood schools, pets, and other personal information about themselves, family, and friends (Furnell, 2008). Subsequently, PII such as names, addresses, demographic characteristics, lifestyle interests, shopping preferences, and purchase histories has become available. Yet it is this type of information that users voluntarily, routinely, and often carelessly divulge in SNS (Phelps et al., 2000; Furnell, 2008).

Despite the risk associated with divulging PII, users increasingly engage with online PISP (Furnell, 2008; Norberg, Horne, & Horne, 2007). For example, some users reveal personal information inadvertently, provide unnecessary personal information, ignore information privacy policies, use the default home network information security settings, open spam email, reply to email spammers, use the same password on multiple accounts, and other risky online practices (Furnell, 2008; Udo, 2001). Moreover, a survey of SNS users revealed 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 (Furnell, 2008). As a result of the immense amount of identifiable personal information users are storing within SNSs, additional research within SNS is warranted.

## Personal Information Sharing in E-learning

In recent years, e-learning has been gaining popularity as another medium to enable efficient knowledge transfer, not only in higher education, but also in business environments (El-Khatib, Korba, Xu, & Yee, 2003; Selim, 2007; Zhang, Zhao, Zhou & Nunamaker, 2004). Additionally, ELS has proliferated as complementary systems for traditional classroom-based training. 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 several types of personal information commonly stored within ELS including personal contact information, learner relationships, learner preferences, learner performance, and portfolios. Consequently, the need for security has become a fundamental requirement of ELS (Levy & Ramim, 2009; Ramim & Levy, 2006; Weippl, 2005).

Many users are opting for e-learning programs, as it facilitates the ability to learn at home or on the go, anytime, and anyplace (Gerkin, Taylor, & Weatherby, 2009). At the same time, users of ELS face an increased risk to their personal information because they are often tempted to provide identifiable personal information to others when interacting via the ELS. The incorporation of ELS into many corporate and academic environments promotes the storage of large identifiable information on third party servers, therefore, increasing the risk to users (Ruiz, Mintzer, & Leipzig, 2006). Many times, such servers can be vulnerable to attacks, any data stolen can be used to commit identity theft, social engineering, and other types of misuses (Hovav & Grey, 2014). This underscores the need to raise awareness among users about their personal information security within ELS (Furnell et al., 2007).

Although SNSs were not created for educational purposes, these can be used to support e-learning activities, while many use SNSs to connect with peers. The success of ELS largely depends on the acceptance of users, as well as use of such systems (Ball & Levy, 2008; Dalsgaard, 2006; 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 poor (El-Khatib et al., 2003; Kritzinger & von Solms, 2006; Webber, Lima, Casa, & Ribeiro,, 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). Researchers indicated that it is essential to protect all ELSs against cyber attacks by installing intrusion detection systems and other security tools. Moreover, the same security considerations that are applied to all other forms of Web-based systems should also be applied to ELS (Ramim & Levy, 2006; Weippl, 2005). These security considerations include confidentiality, integrity, and availability (Weippl, 2005). Security is potentially one of the most important considerations when developing and deploying ELS (Webber et al., 2007).

## Purpose of the Study

The purpose of this study was to empirically assess the influence of users' PISA on PISH, and PISP, as well as compare the three constructs between SNS and ELS. Based on this purpose, the following hypotheses (noted in hull form) were addressed:

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.

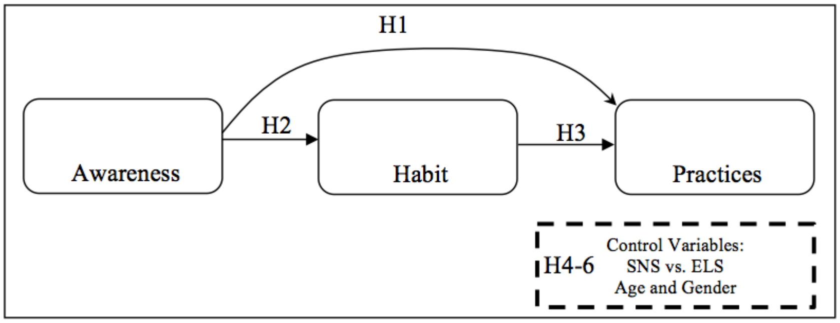

**Figure 1.** The Conceptual Map of Awareness, Habit, and Practices in the context of Personal Information Sharing

# Methodology

This study was an empirical study, as it empirically assessed the proposed contributions along with testing the differences in users' PISA, PISH, and PISP between SNS and ELS. This study used a survey methodology, and collected data through a Web-enabled survey instrument administered to students and faculty members.

## 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."

### *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, Kremers, Singh, van den Putte, & van Mechelen (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), while used a five-point Likert scale for measuring PISH. The specific items, numbered PISH1 through PISH12.

### *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.

## Validity and Reliability

Instrument validation is a crucial requirement of research (Straub, 1989). Validity is used to measure the level to which the instrument indeed measures the proposed measurement. In the context of causal research, internal validity is the degree of confidence the researcher has (Sekaran, 2003). According to Straub (1989), literature reviews and expert panels establish content validity. 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. External validity allows researchers to generalize the findings of investigations to other environments (Straub, Rai, & Klein, 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.

Establishing reliability within research is the process of documenting internal consistency (Sekaran, 2003; Straub, 1989; Straub et al., 2004). 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 .70 being the lowest acceptable limited of the measure, and 1.0 nearing outmost reliability (Gefen, Straub, & Boudreau, 2000). 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 performed on each set of construct's 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. Following, path analysis was preformed to address H1, H2, and H3, whereas Analysis of Covariance (ANCOVA) was used to address H4, H5, and H6. Additional details about the specific analyses used are outlines as part of the results and data analyses section below.

# Data Analyses and Results

## Study Participants

Following the expert panel review and minor wording adjustments, the final draft survey was administered to 2,159 students and 221 faculty members. Useable response included 296 students and 94 faculty members. Thus, the response rate was 13.9% for students and 42.9% for faculty. Table 1 represents the results by gender, age, marital status, and education level.

Table 1. Study Participants 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% |
| ***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% |

| Item | Frequency | Percentage |
|---|---|---|
| ***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% |

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.

## Reliability Analysis of Constructs

After completing pre-analysis screening using Statistical Package for Social Sciences (SPSS), the data was examined for outliers, with two responses removed from the final data set due to extreme multivariate outliers, leaving 390 usable responses for further analysis. Next, the reliability of the instrument was verified through Cronbach's Alpha. The Cronbach's Alpha coefficients were: 0.891, 0.913, .911 for PISA, PISH, and PISP respectively for the ELS constructs, as well as 0.877, 0.912, and 0.947 for PISA, PISH, and PISP respectively for the SNS constructs.

## Path Analysis

Path analysis was used to estimate causal relations among several variables (Mertler & Vanatta, 2010). Results of this research fail to reject H1a and H1b, and suggested that users' PISA had no significant effect on their PISP in either SNS or ELS. Results also fail to reject H2a and H2b, and suggested that users' PISA also had no significant effect on their PISH in either SNS or ELS. However, H3a and H3b were not supported, as PISH was found to have a significant ($p<.0001$) effect on PISP, in both SNS and ELS. These results indicated that habit was the strongest indicator of users' practices. Results of the path analysis for the SNS and ELS are provided in Figures 2 and 3 respectively.

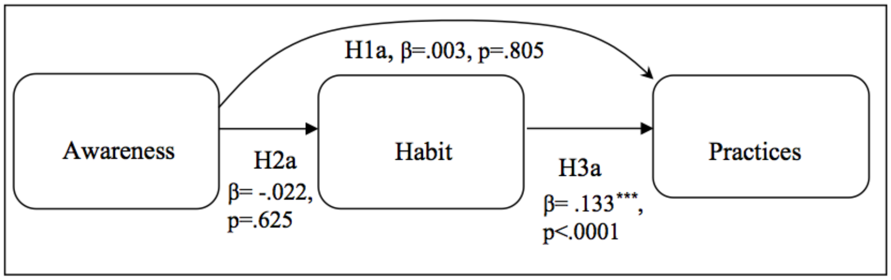

**Figure 2.** Conceptual Model for SNS

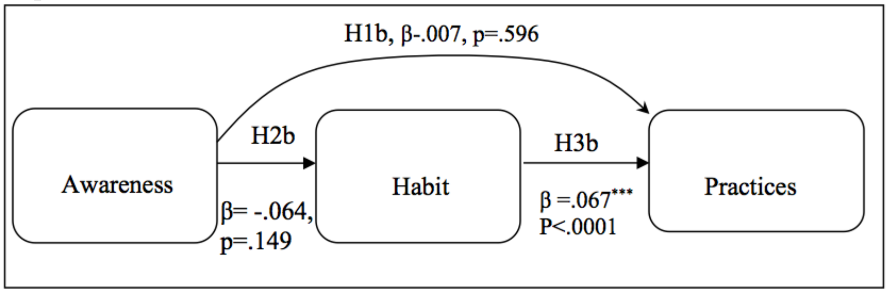

**Figure 3.** Conceptual Model for ELS

## Analysis of Covariance (ANCOVA)

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 regarding PISA, PISH, and PISP between the SNS and ELS environments, when controlling for gender as well as age. 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). ANCOVA results indicated that there were no significant main effect in users' PISA between the SNS and ELS environments, when controlling for gender (F(1, 388)=.293, p=.589, partial $\eta^2$=0.001), as well as age (F(1, 388)=.020, p=.888, partial $\eta^2$<0.001). Moreover, results indicated that there were significant main effect in users' PISH between SNS or ELS when controlling for gender (F(1, 388)=5.037, p=.025, partial $\eta^2$=0.013), as well as age (F(1, 388)=29.57, p<.0001, partial $\eta^2$=0.071). Additionally, results indicated that there was marginally significant main effect in users' PISP between SNS or ELS when controlling for gender (F(1, 388)=3.77, p=.053, partial $\eta^2$=0.01), while full significant main effect in users' PISP between SNS or ELS when controlling for age (F(1, 388)=28.95, p<.001, partial $\eta^2$=0.072). Table 2 provides a summary of all results.

Table 2. Summary of Hypotheses Results

| | |
|---|---|
| Ho1a: There will be no statistically significant effect of SNS users’ PISA on their PISP. | Failed to reject<br>(p=.805) |
| Ho1b: There will be no statistically significant effect of ELS users’ PISA on their PISP. | Failed to reject<br>(p=.596) |
| Ho2a: There will be no statistically significant effect of SNS users’ PISA on their PISH. | Failed to reject<br>(p=.625) |
| Ho2b: There will be no statistically significant effect of ELS users’ PISA on their PISH. | Failed to reject<br>(p=.149) |
| Ho3a: There will be no statistically significant effect of SNS users’ PISH on their PISP. | Rejected<br>(p<.0001) |
| Ho3b: There will be no statistically significant effect of ELS users’ PISH on their PISP. | Rejected<br>(p<.0001) |
| Ho4a: There will be no statistically significant difference between users’ PISA within SNS and users’ PISA within ELS, when controlling for gender. | Failed to reject<br>(p=.589) |
| Ho4b: There will be no statistically significant difference between users’ PISA within SNS and users’ PISA within ELS, when controlling for age. | Failed to reject<br>(p=.888) |
| Ho5a: There will be no statistically significant difference between users’ PISH within SNS and users’ PISH within ELS, when controlling for gender. | Rejected<br>(p=.025) |
| Ho5b: There will be no statistically significant difference between users’ PISH within SNS and users’ PISH within ELS, when controlling for age. | Rejected<br>(p<.0001) |
| Ho6a: There will be no statistically significant difference between users’ PISP within SNS and users’ PISP within ELS, when controlling for gender. | Partially reject<br>(p=.053) |
| Ho6b: There will be no statistically significant difference between users’ PISP within SNS and users’ PISP within ELS, when controlling for age. | Rejected<br>(p<.001) |

## Conclusion and Discussions

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. Based on measures from prior literature, a quantitative survey instrument was developed. Then, an expert panel evaluated the instrument. Results of the expert panel provided some minor wording and item structure adjustments to improve survey readability. Following approval from the Institutional Review Board (IRB), the anonymous quantitative survey was sent to both all faculty members and students at a small private university in southeast United States. Then, the date collected was reviewed for assumptions and multivariate outliers, resulting in 390 usable records.

Cronbach’s Alpha of all constructs was very high ranging from 0.877 to 0.947 indicating strong construct reliability for the measures. Results of the path analysis indicated that awareness was not significantly influencing habit or practices. However, habit was found to significantly influence practices, suggesting that additional studies need to better understand the strengths between habit and practices, along with the predecessors of habit. The results of study suggest that habit is the strongest contributor to users’ information sharing activities. Thus, a strong framework for personal information security within the SNS and ELS environments is supported in this study. Awareness of personal information security risks does not necessarily produce better personal information sharing practices. Rather, educating users and helping them to establish safer habits and practices can reduce the risks associated with exposing personal identifiable information is SNSs and ELS.

ANCOVA was used to determined if there are any significant main effect in users' PISA, PISH, and PISP between the SNS as well as ELS environments, when controlling for gender and age. Results of the awareness test indicated that there was no statistically significant main effect 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). Results of the habit test indicated that there was statistically significant main effect between users' PISH in either SNS or ELS environments, when controlling for gender or age. These findings are 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 et al., 2010; Yeh, 2009). As such, we assume that the results are context related, and additional research, especially in the context of information sharing via other types of systems is warranted. Furthermore, results of the practice test indicated mixed findings between users' PISP in either SNS or ELS environments, when controlling for gender or age. Specifically, ANCOVA results suggested that there was marginally significant main effect (p=0.053) between users' PISP in either SNS or ELS, when controlling for gender. These findings are consistent with literature that provided evidences of contradicting results, some suggests that gender does not have an effect on users' practices (Dinev & Hart, 2006; Furnell, 2008; Levy & Ramim, 2009; Power & Trope, 2006), while others such as Fogel and Nehmad (2009), suggested gender does affect users' online personal information sharing practices. These findings do provide fruitful grounds for additional research as it is still evident that the results are mixed, and may be due to the difference in the participants' demographics as well as context of the research. For example, the participants in this study were older than those in the Fogel and Nemad (2009) study, with a greater percentage of females. Finally, MANCOVA results suggested that there was a statistically significant main effect between users' 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.

This study included three main limitations, namely: the sample response rate, sample average age, and gender distribution. First limitation of this study deals with the sample that was collected from a small private university in the Southeast United States. The overall response rate was relatively small, with a rate of 16%. The sample comprised of non-traditional adult students and faculty members. Further research is warrant in different geographical regions with traditional diversified student body. The second limitation is associated with sample comprising of older participants, 53% of the students were 35 years or older, and 71% of the faculty were older than 40 years. Younger populations may have different PISP compared to an older population. The third limitation is associated with the gender distribution where majority of the study participants where females, 68% of students, and 53% of faculty members, as it appears that significantly more females were willing to participate in the study than males. This also requires careful attention in follow up research to ensure incentives are provided to allure more males to participate in the research.

Future research should focus on investigating the effect of awareness training to further the insight into how PISA, PISH, and PISP interact to influence users' online sharing of personal information via an experimentation type study. Moreover, while measuring perceptions have long been documented in literature to provide good indications of actual behaviors, additional research may look into the actual measures of awareness, habits, and practices by observations or other techniques to further investigate such interaction.

## Acknowledgments

We would like to thank the anonymous referees for their careful review and valuable suggestions. We also would like to thank the accepting editor, Dr. Alex Koohang, for his recommendations and constructive comments. Moreover, we would like to thank the Knowledge Management (KM) Conference 2015 program chair, Dr. Nitza Geri, for her guidance and thoughtful comments. Thank you all!

## 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.

Asanka, N., Arachchilage, G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior, 29*, 706-714.

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 June 29, 2014 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.

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

Burley, D. L., Eisenberg, J., & Goodman, S. E. (2015). Privacy and security: Would ccybersecurity professionalization help address the cybersecurity crisis? *Communications of ACM, 57*(2), 24-27.

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

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

Dalsgaard, C. (2006). Social software: E-learning beyond learning management systems. *European Journal of Open, Distance and E-learning*, *2006*(II). Retrieved June 28, 2014 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., 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.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79-98.

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

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.

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.

Hovav, A., & Gray, P. (2014). The ripple effect of an information security breach event: A stakeholder analysis. *Communications of the Association for Information Systems, 34*(1), 893-912.

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.

Krigsman, M. (2009). Hackers program highway sign with Zombie warning. *ZDnet.com*. Retrieved July 13, 2014 from http://www.zdnet.com/article/hackers-program-highway-sign-with-zombie-warning/

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., & 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.

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.

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.

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.

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.

Polites, G. L., & Karahanna, E. (2012). Shackled to the status quo: the inhibiting effects of incumbent system habit, switching costs, and inertia on new system acceptance. *MIS Quarterly, 36*(1), 21-42

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.

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.

Shakespeare, Othello, 1996. 3.3.

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.

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, Florida, 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, 2014 from http://www.cmsturgeon.com/itconf/facebook-report.pdf

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.

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.

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

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.

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.*

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.

# Appendix – The Survey Instrument

**1. 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©**

| No. | Item | | | | | |
|---|---|---|---|---|---|---|
| PISA_SN1. | To what extent do you think that Facebook© shares your personal information with other companies? | Not at all<br>(1) | Slightly<br>(2) | Moderately<br>(3) | Very<br>(4) | Extremely<br>(5) |
| PISA_SN2. | To what extent do you think about your personal information being shared by Facebook©? | Not at all<br>(1) | Slightly<br>(2) | Moderately<br>(3) | Very<br>(4) | Extremely<br>(5) |
| PISA_SN3. | To what extent do you think that other individuals use any information you provided on Facebook©? | Not at all<br>(1) | Slightly<br>(2) | Moderately<br>(3) | Very<br>(4) | Extremely<br>(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<br>(1) | Slightly<br>(2) | Moderately<br>(3) | Very<br>(4) | Extremely<br>(5) |

**2. 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©:**

| No. | Item | | | | | |
|---|---|---|---|---|---|---|
| PISA_EL1. | To what extent do you think your university shares your personal information posted on Blackboard© with other companies? | Not at all<br>(1) | Slightly<br>(2) | Moderately<br>(3) | Very<br>(4) | Extremely<br>(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<br>(1) | Slightly<br>(2) | Moderately<br>(3) | Very<br>(4) | Extremely<br>(5) |
| PISA_EL3. | To what extent do you think that other individuals use any information you provided on Blackboard©? | Not at all<br>(1) | Slightly<br>(2) | Moderately<br>(3) | Very<br>(4) | Extremely<br>(5) |
| PISA_EL4. | To what extent do you think about your personal information provided on Blackboard© being shared by employees at the university? | Not at all<br>(1) | Slightly<br>(2) | Moderately<br>(3) | Very<br>(4) | Extremely<br>(5) |

**3. 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©**

| No. | Item | Facebook© | | | | | Blackboard© | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 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) |
| 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) |

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

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

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

| No. | Item | | |
|---|---|---|---|
| IDT1. | You have personally been a victim of identity theft or other unauthorized use of your personal information | Yes<br>☐ | No<br>☐ |
| IDT2. | Someone in your family has been a victim of identity theft or other unauthorized use of their personal information | Yes<br>☐ | No<br>☐ |
| IDT3. | Someone in your workplace or school has been a victim of identity theft or other unauthorized use of their personal information | Yes<br>☐ | No<br>☐ |

**6. 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 | ☐ Vocational 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**<br>☐ | **NO**<br>☐ |

**If no please explain**

| | | |
|---|---|---|
| **2. Do the items appropriately measure the construct being evaluated?** | **YES**<br>☐ | **NO**<br>☐ |

**If no please explain**

| | | |
|---|---|---|
| **3. Are there items that you would recommend revising?** | **YES**<br>☐ | **NO**<br>☐ |

**If yes please explain**

| | | |
|---|---|---|
| **4. Would you recommend deleting any items?** | **YES**<br>☐ | **NO**<br>☐ |

**If yes please explain**

| | | |
|---|---|---|
| **5. Would you recommend including any additional items in this proposed instrument?** | **YES**<br>□ | **NO**<br>□ |

**If yes please explain**

| | | |
|---|---|---|
| **6. Any general comments?** | **YES**<br>□ | **NO**<br>□ |

**If yes, please provide here**

## Authors' Biographies

**Albert L. Ball, Ph.D.** is the Dean of the Fisher School of Technology, Hodges University in Naples Florida. Dr. Ball retired from the U.S. Navy. He has a Ph.D. in Information Systems from Nova Southeastern University. He also holds a Master of Science degree in Computer Information Systems from Hodges University, with an emphasis in Networking Technology. He has worked in the technology industry for 20 years, holding several positions including network administration, database administration, PC technician, and programmer. He has published referee articles in several conference proceedings. Additionally, Dr. Ball is currently serving on the editorial review board for the International Institute for Applied Knowledge Management Journal. He is also serving as an adviser to the Clute Institute as well as a reviewer for the Business Information Systems Journal. He also holds the following certifications: A+, Network+, MCP, CCNA, CNA, iNet+.

**Yair Levy, Ph.D.** is a Professor of Information Systems and Cybersecurity at the Graduate School of Computer and Information Sciences, Nova Southeastern University and the director of the Center for e-Learning Security Research (CeLSR). During the mid to late 1990s, he assisted NASA to develop e-learning systems.  He earned his Bachelor's degree in Aerospace Engineering from the Technion (Israel Institute of Technology). He received his MBA with MIS concentration and Ph.D. in Management Information Systems from Florida International University. His current research interests include security issues with cybersecurity skills and competencies, user-authentication, information privacy, and e-learning systems security, as well as social engineering awareness and cyber threat prevention. His research publications appear in numerous peer-reviewed journals and conference proceedings. Also, Dr. Levy has been serving as a member of conference proceedings committee for numerous scholarly conferences. Moreover, Dr. Levy has been serving as a referee research reviewer for hundreds of national and international scientific outlets. He is a frequent invited keynote speaker at national and international meetings on cybersecurity, IS, and online learning topics. Dr. Levy's teaching interests in the masters level include information systems security, e-commerce, and Web development. His teaching interests in the doctoral level include Information Security Risk Management and Advanced Multivariate Research Methods and Statistics. To find out more about Dr. Levy, please visit his site: http://scis.nova.edu/~levyy/.

**Michelle M. Ramim, Ph.D.** is an Associate Professor at the Fisher School of Technology, Hodges University. She has extensive experience in information technology (IT) consulting. Dr. Ramim directed the development and implementations of several IT projects including promotional and interactive websites for major enterprises such as Debeer (Diamond Trading Company). Her current research interests include ethical issues with IT, information security and crisis management, privacy and legal aspects of computing, as well as ethical decision making. She has published articles in peer-reviewed outlets including journals, conference proceedings, encyclopedias, and an invited chapter. A number of her papers won the 'best paper' award in national and international peer-review conference proceedings. Moreover, she has been serving as a referee research reviewer for national and international scientific journals, conference proceedings, as well as management information systems textbooks. She has developed the supplemental material for the Pearlson and Saunders (2012) 5th ed. book “Managing and Using Information Systems: A Strategic Approach” by Wiley & Sons. She earned her Bachelor’s degree from Barry University in Miami, Florida. Dr. Ramim has received her Executive MBA from Florida International University. She completed her Ph.D. in Information Systems at the Graduate School of Computer and Information Sciences, Nova Southeastern University.